VASCO THE AUTHENTICATION COMPANY

DIGIPASS Authentication for WatchGuard Firebox

With Vasco VACMAN Middleware 3.0

Integration Guideline

Disclaimer

Disclaimer of Warranties and Limitations of Liabilities
This Report is provided on an 'as is' basis, without any other warranties, or conditions.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of VASCO Data Security.

Trademarks
DIGIPASS & VACMAN are registered trademarks of VASCO Data Security. All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.

Copyright
© 2006 VASCO Data Security. All rights reserved.

Table of Contents

DIGIPASS Authentication for WatchGuard Firebox 1

Disclaimer 2

Table of Contents 3

1 Overview 5

2 Problem Description 5

3 Solution 5

4 Technical Concept 6

4.1 General overview 6

4.2 WatchGuard Firebox prerequisites 6

4.3 VACMAN Middleware Prerequisites 6

5 WatchGuard Firebox 7

5.1 WatchGuard Firebox configuration 7

5.2 Authentication Servers 10

5.3 Authentication Policy 11

5.4 Website Proxy Policy 12

5.5 Saving Changes 18

6 VACMAN Middleware 19

6.1 Configure VACMAN Middleware 19

7 Microsoft IAS 24

8 User configuration 33

8.1 ODBC installation 33

8.1.1 User creation 33

8.1.2 Import DIGIPASS 35

8.1.3 DIGIPASS Assignment 37

8.2 Active Directory installation 39

8.2.1 User creation 39

8.2.2 Import DIGIPASS 41

8.2.3 DIGIPASS assignment 43

9 Firebox Authentication Test 45

9.1 Response Only 46

9.2 Challenge/Response 48

10 VACMAN Middleware features 50

10.1 Installation 50

10.1.1 Support for Windows 2000, 2003, IIS5 and IIS6 50

10.1.2 Support for ODBC databases and Active Directory 50

10.2 Deployment 50

10.2.1 Dynamic User Registration (DUR) 50

10.2.2 Autolearn Passwords 50

10.2.3 Stored Password Proxy 50

10.2.4 Authentication Methods 50

10.2.5 Policies 51

10.2.6 DIGIPASS Self Assign 51

10.2.7 DIGIPASS Auto Assign 51

10.2.8 Grace Period 51

10.2.9 Virtual DIGIPASS 51

10.3 Administration 52

10.3.1 Active Directory Users and Computers Extensions 52

10.3.2 Administration MMC Interface 52

10.3.3 User Self Management Web Site 53

10.3.4 Delegated administration 53

10.3.5 Granular access rights 53

11 About VASCO Data Security 54

1 Overview

The purpose of this document is to demonstrate how to configure VACMAN Middleware (VM) to work with the WatchGuard Firebox. The Firebox will be deployed as the companies firewall in the DMZ zone, connecting and protecting different internal networks.

2 Problem Description

The basic working of the Firebox is based on authentication to an existing media (LDAP, Radius, local authentication …). To use the VACMAN Middleware with the Firebox, its RADIUS settings need to be changed or added manually.

3 Solution

After configuring VACMAN Middleware and the Firebox in the right way, you eliminate the weakest link in any security infrastructure – the use of static passwords – that are easily stolen guessed, reused or shared. The Firebox also enables you to work with group options in their firewall.

In this Integration Guide we will secure a corporate website. So everyone, coming from the External network (Internet), will have to authenticate before access will be granted to the website. We will use a WatchGuard Firebox Peak X8000.

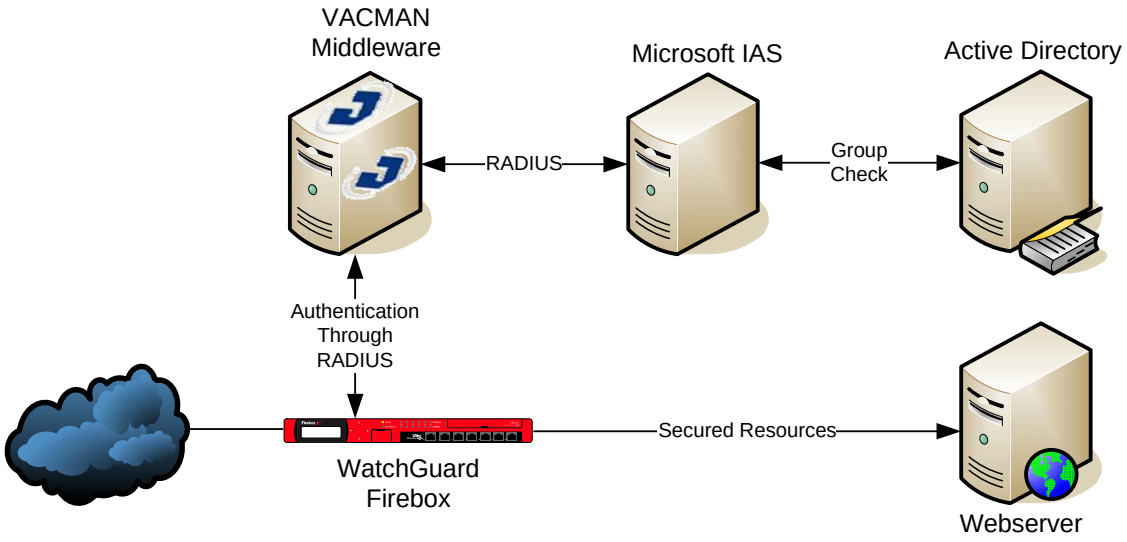


Figure 1: Solution

4 Technical Concept

4.1 General overview

The main goal of the WatchGuard Firebox is to perform authentication to secure all kind of firewall connections. As the WatchGuard Firebox can do authentication to an external service with RADIUS, we will place the VACMAN Middleware as middleware or as back-end service, to secure the authentication with our proven VACMAN Middleware software.

We will also show you how to setup a group authentication based on Active Directory security groups, in combination with Microsoft Internet Authentication Service (IAS).

4.2 WatchGuard Firebox prerequisites

Please make sure you have a working setup of the WatchGuard Firebox. It is very important this is working correctly before you start implementing the authentication to the VM.

Any WatchGuard Firebox X Core or Peak with Fireware 8.3 or Fireware Pro 8.3 will be supported by this integration guide.

We used for our tests a Firebox X8000 Peak running Fireware Pro 8.3.

4.3 VACMAN Middleware Prerequisites

In this guide we assume you already have VACMAN Middleware 3.0 (VM) installed and working. If this is not the case, make sure you get VM working before installing any other features.

5 WatchGuard Firebox

5.1 WatchGuard Firebox configuration

To change the settings on the Firebox you need to connect to the Firebox through the WatchGuard System Manager. Click on the **Connect to device** button.

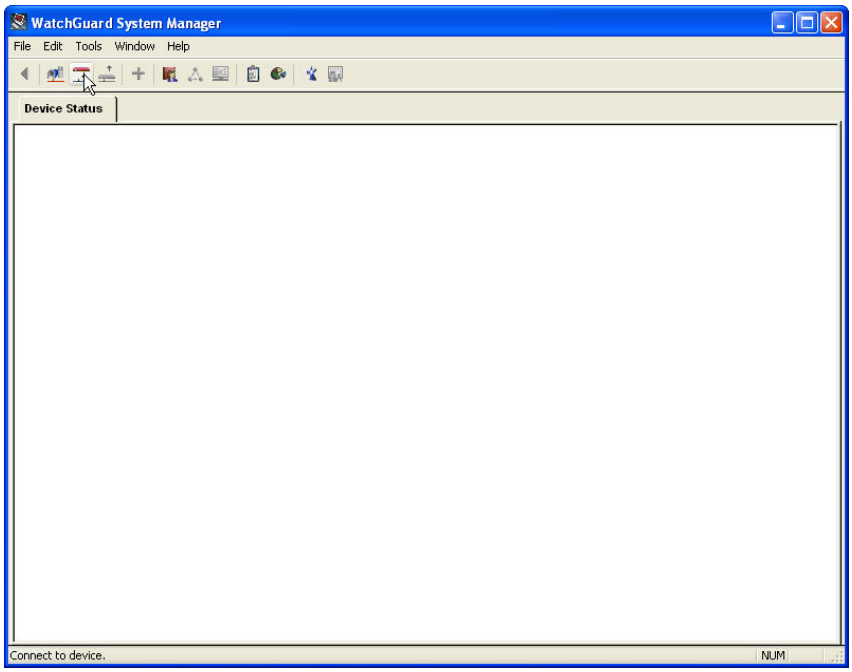


Figure 2: WatchGuard Firebox configuration (1)

Enter the **hostname or IP address** of the WatchGuard Firebox and the **read/status passphrase** of the device. Click **Login** to continue.

Note: The read/status passphrase only allows you to view the settings of the Firebox, it's not possible to make changes with this passphrase.

Figure 3: WatchGuard Firebox configuration (2)

Once connected, you can view the status of the Firebox. Click on the **Policy Manager** button to view the policy details.

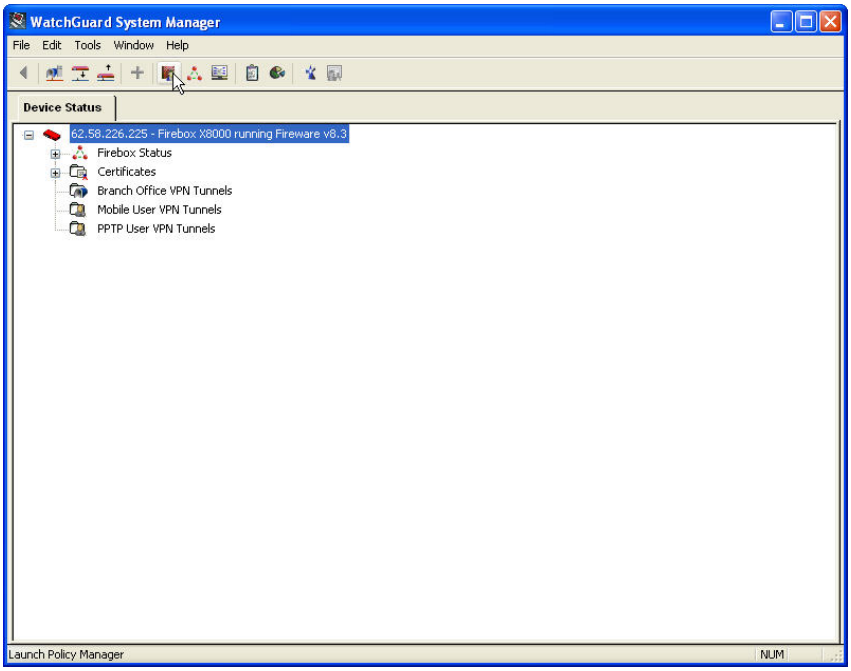


Figure 4: WatchGuard Firebox configuration (3)

The following screen (Figure 5) shows you an overview of the policies already present in the firebox. A more detailed view is available by right clicking the window and selecting **Detailed View**.

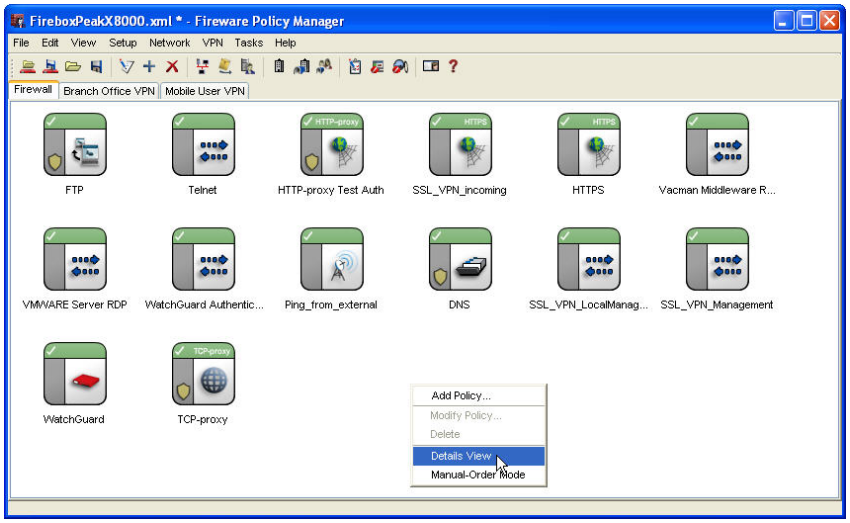


Figure 5: WatchGuard Firebox configuration (4)

This way you get a better insight of all the rules present in the Firebox. To view the network settings, you can open **Network – Configuration …**

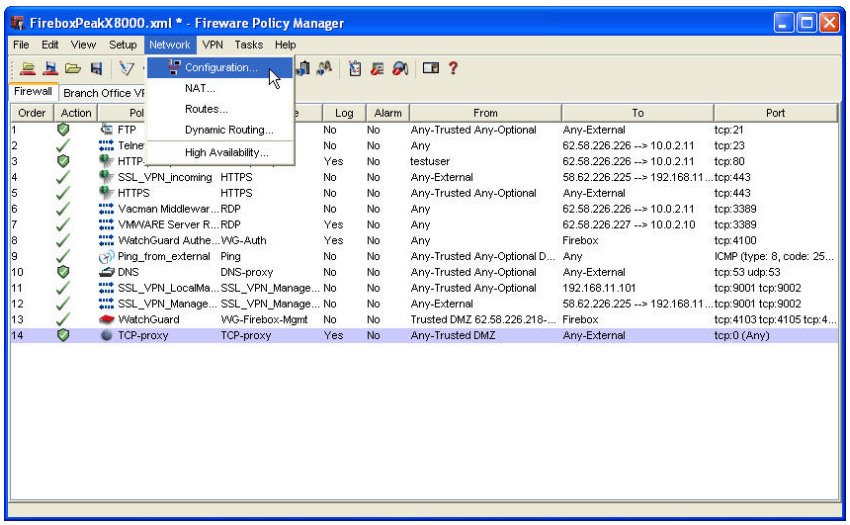

FireboxPeakX8000.xml * - Fireware Policy Manager
File Edit View Setup Network VPN Tasks Help
Configuration...
NAT...
Routes...
Dynamic Routing...
High Availability...
Firewall Branch Office VP
Order Action Pol Log Alarm From To Port
1 FTP No No Any-Trusted Any-Optional Any-External tcp:21
2 Telne No No Any 62.58.226.226 --> 10.0.2.11 tcp:23
3 HTTP- Yes No testuser 62.58.226.226 --> 10.0.2.11 tcp:80
4 SSL_VPN_incoming HTTPS No No Any-External 58.62.226.225 --> 192.168.11... tcp:443
5 HTTPS HTTPS No No Any-Trusted Any-Optional Any-External tcp:443
6 Vacman Middlewar... RDP No No Any 62.58.226.226 --> 10.0.2.11 tcp:3389
7 VMWARE Server R... RDP Yes No Any 62.58.226.227 --> 10.0.2.10 tcp:3389
8 WatchGuard Authe... WG-Auth Yes No Any Firebox tcp:4100
9 Ping_from_external Ping No No Any-Trusted Any-Optional D... Any ICMP (type: 8, code: 25...
10 DNS DNS-proxy No No Any-Trusted Any-Optional Any-External tcp:53 udp:53
11 SSL_VPN_LocalMa... SSL_VPN_Manage... No No Any-Trusted Any-Optional 192.168.11.101 tcp:9001 tcp:9002
12 SSL_VPN_Manage... SSL_VPN_Manage... No No Any-External 58.62.226.225 --> 192.168.11... tcp:9001 tcp:9002
13 WatchGuard WG-Firebox-Mgmt No No Trusted DMZ 62.58.226.218-... Firebox tcp:4103 tcp:4105 tcp:4...
14 TCP-proxy TCP-proxy Yes No Any-Trusted DMZ Any-External tcp:0 (Any)

Figure 6: WatchGuard Firebox configuration (5)

Make sure all network elements are configured correctly as the rules rely on the names you gave your network elements.

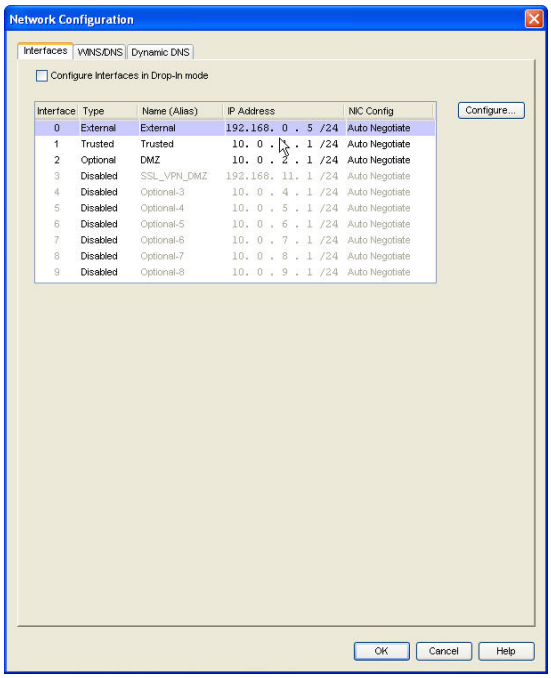

Network Configuration
Interfaces WINS/DNS Dynamic DNS
Configure Interfaces in Drop-In mode
Interface Type Name (Alias) IP Address NIC Config
0 External External 192.168. 0 . 5 /24 Auto Negotiate
1 Trusted Trusted 10. 0 . 1 . 1 /24 Auto Negotiate
2 Optional DMZ 10. 0 . 2 . 1 /24 Auto Negotiate
3 Disabled SSL_VPN_DMZ 192.168. 11. 1 /24 Auto Negotiate
4 Disabled Optional-3 10. 0 . 4 . 1 /24 Auto Negotiate
5 Disabled Optional-4 10. 0 . 5 . 1 /24 Auto Negotiate
6 Disabled Optional-5 10. 0 . 6 . 1 /24 Auto Negotiate
7 Disabled Optional-6 10. 0 . 7 . 1 /24 Auto Negotiate
8 Disabled Optional-7 10. 0 . 8 . 1 /24 Auto Negotiate
9 Disabled Optional-8 10. 0 . 9 . 1 /24 Auto Negotiate
Configure...
OK Cancel Help

Figure 7: WatchGuard Firebox configuration (6)

5.2 Authentication Servers

Click on the **Authentication servers** button to open the authentication options. Here we will be able to add the RADIUS server details.

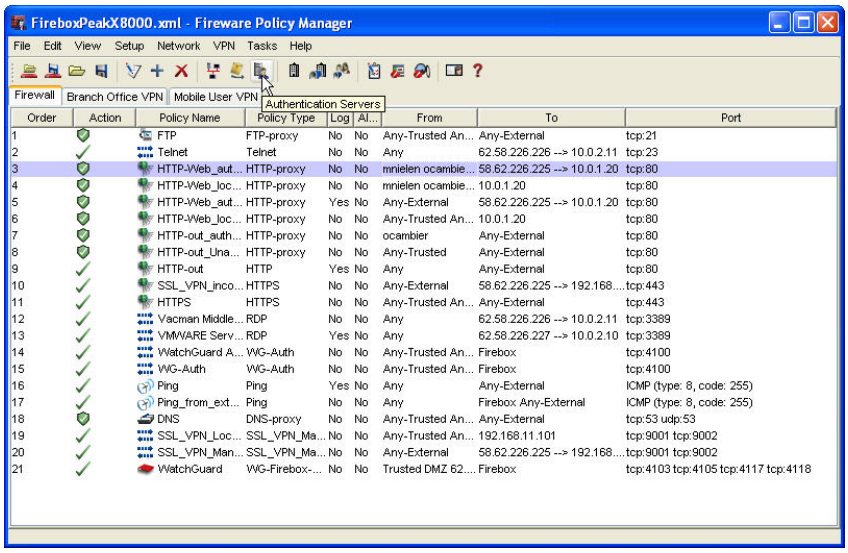

FireboxPeakX8000.xml - Fireware Policy Manager
File Edit View Setup Network VPN Tasks Help
Authentication Servers
Firewall Branch Office VPN Mobile User VPN
Order Action Policy Name Policy Type Log Al... From To Port
1 FTP FTP-proxy No No Any-Trusted An... Any-External tcp:21
2 Telnet Telnet No No Any 62.58.226.226 --> 10.0.2.11 tcp:23
3 HTTP-Web_aut... HTTP-proxy No No mnielen ocambie... 58.62.226.225 --> 10.0.1.20 tcp:80
4 HTTP-Web_loc... HTTP-proxy No No mnielen ocambie... 10.0.1.20 tcp:80
5 HTTP-Web_aut... HTTP-proxy Yes No Any-External 58.62.226.225 --> 10.0.1.20 tcp:80
6 HTTP-Web_loc... HTTP-proxy No No Any-Trusted An... 10.0.1.20 tcp:80
7 HTTP-out_auth... HTTP-proxy No No ocambier Any-External tcp:80
8 HTTP-out_Una... HTTP-proxy No No Any-Trusted Any-External tcp:80
9 HTTP-out HTTP Yes No Any Any-External tcp:80
10 SSL_VPN_inco... HTTPS No No Any-External 58.62.226.225 --> 192.168... tcp:443
11 HTTPS HTTPS No No Any-Trusted An... Any-External tcp:443
12 Vacman Middle... RDP No No Any 62.58.226.226 --> 10.0.2.11 tcp:3389
13 VMWARE Serv... RDP Yes No Any 62.58.226.227 --> 10.0.2.10 tcp:3389
14 WatchGuard A... WG-Auth No No Any-Trusted An... Firebox tcp:4100
15 WG-Auth WG-Auth No No Any-Trusted An... Firebox tcp:4100
16 Ping Ping Yes No Any Any-External ICMP (type: 8, code: 255)
17 Ping_from_ext... Ping No No Any Firebox Any-External ICMP (type: 8, code: 255)
18 DNS DNS-proxy No No Any-Trusted An... Any-External tcp:53 udp:53
19 SSL_VPN_Loc... SSL_VPN_Ma... No No Any-Trusted An... 192.168.11.101 tcp:9001 tcp:9002
20 SSL_VPN_Man... SSL_VPN_Ma... No No Any-External 58.62.226.225 --> 192.168... tcp:9001 tcp:9002
21 WatchGuard WG-Firebox-... No No Trusted DMZ 62.... Firebox tcp:4103 tcp:4105 tcp:4117 tcp:4118

Figure 8: Authentication Servers (1)

Go to the RADIUS tab and fill in the details of the VACMAN Middleware server. IP address, Port (default 1812), (shared) secret and confirmation. The timeout and Retry fields are optional. The Group Attribute must contain value 11. This will be the field that receives information about the group name by IAS.

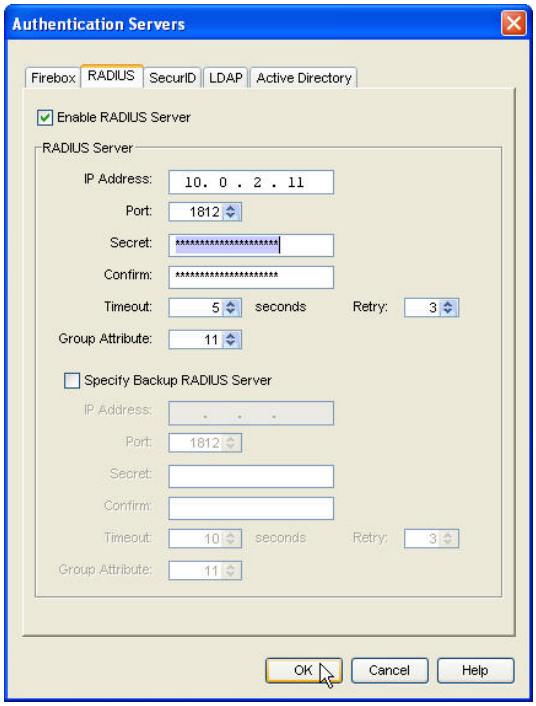


Figure 9: Authentication Servers (2)

5.3 Authentication Policy

To authenticate on the Firebox, it is necessary you are allowed to see the authentication page. Find the rule **WatchGuard Authentication**. Check if the permissions are:

FROM: **Any** TO: **Firebox** PORT: **tcp:4100**.

If they do not match, please follow the steps below to change them.

Right-click the WatchGuard Authentication rule and select **Modify Policy…** .

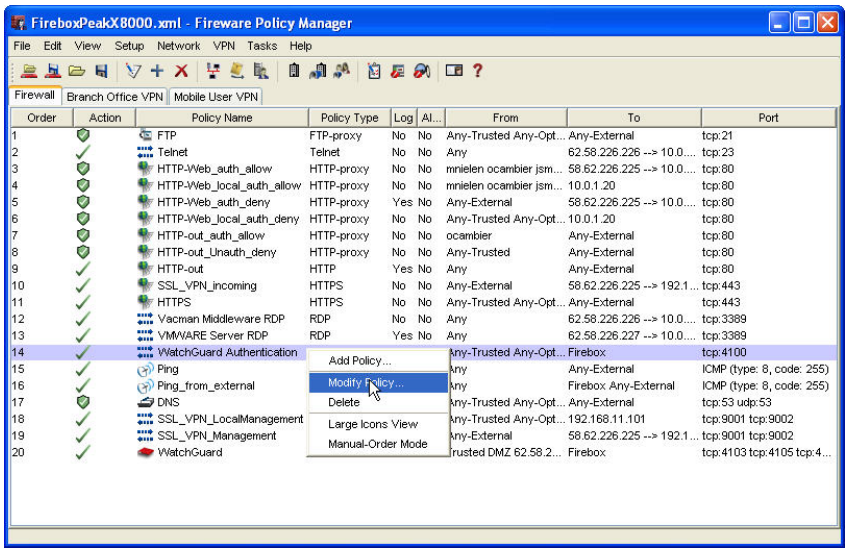

FireboxPeakX8000.xml - Fireware Policy Manager
File Edit View Setup Network VPN Tasks Help
Firewall Branch Office VPN Mobile User VPN
Order Action Policy Name Policy Type Log Al... From To Port
1 FTP FTP-proxy No No Any-Trusted Any-Opt... Any-External tcp:21
2 Telnet Telnet No No Any 62.58.226.226 --> 10.0.... tcp:23
3 HTTP-Web_auth_allow HTTP-proxy No No mnielen ocambier jsm... 58.62.226.225 --> 10.0.... tcp:80
4 HTTP-Web_local_auth_allow HTTP-proxy No No mnielen ocambier jsm... 10.0.1.20 tcp:80
5 HTTP-Web_auth_deny HTTP-proxy Yes No Any-External 58.62.226.225 --> 10.0.... tcp:80
6 HTTP-Web_local_auth_deny HTTP-proxy No No Any-Trusted Any-Opt... 10.0.1.20 tcp:80
7 HTTP-out_auth_allow HTTP-proxy No No ocambier Any-External tcp:80
8 HTTP-out_Unauth_deny HTTP-proxy No No Any-Trusted Any-External tcp:80
9 HTTP-out HTTP Yes No Any Any-External tcp:80
10 SSL_VPN_incoming HTTPS No No Any-External 58.62.226.225 --> 192.1... tcp:443
11 HTTPS HTTPS No No Any-Trusted Any-Opt... Any-External tcp:443
12 Vacman Middleware RDP RDP No No Any 62.58.226.226 --> 10.0.... tcp:3389
13 VMWARE Server RDP RDP Yes No Any 62.58.226.227 --> 10.0.... tcp:3389
14 WatchGuard Authentication Any-Trusted Any-Opt... Firebox tcp:4100
15 Ping Any Any-External ICMP (type: 8, code: 255)
16 Ping_from_external Any Firebox Any-External ICMP (type: 8, code: 255)
17 DNS Any-Trusted Any-Opt... Any-External tcp:53 udp:53
18 SSL_VPN_LocalManagement Any-Trusted Any-Opt... 192.168.11.101 tcp:9001 tcp:9002
19 SSL_VPN_Management Any-External 58.62.226.225 --> 192.1... tcp:9001 tcp:9002
20 WatchGuard rusted DMZ 62.58.2... Firebox tcp:4103 tcp:4105 tcp:4...
Add Policy...
Modify Policy...
Delete
Large Icons View
Manual-Order Mode

Figure 10: Authentication Policy (1)

You will receive an information message stating that the policy you want to edit is an automatically generated policy. Click **Yes** to continue.

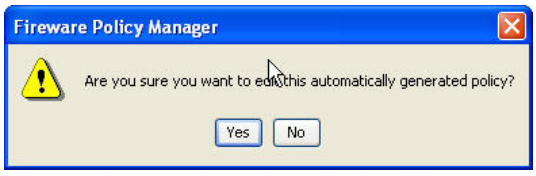


Figure 11: Authentication Policy (2)

In the *From:* field add **Any** and in the *To:* field add **Firebox**. Click OK to complete.

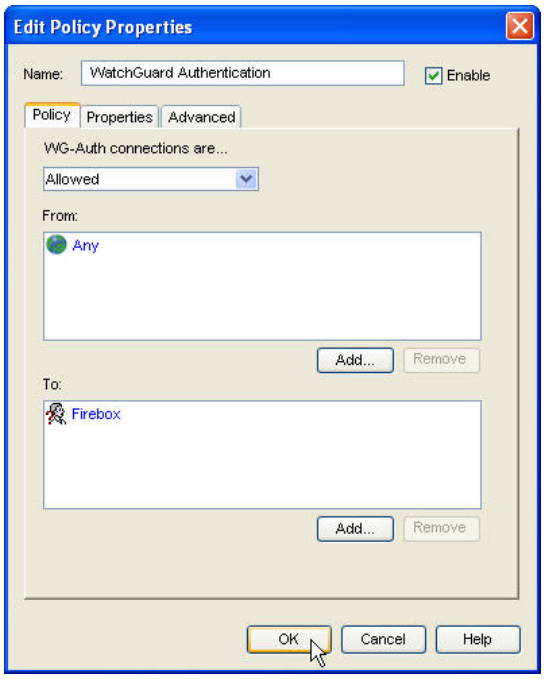


Figure 12: Authentication Policy (3)

5.4 Website Proxy Policy

The actual event we want secure, is when a user requests a website that may not be visited by other people then your own employees. So we will create a rule for this.

Click the **Add Policies** button.

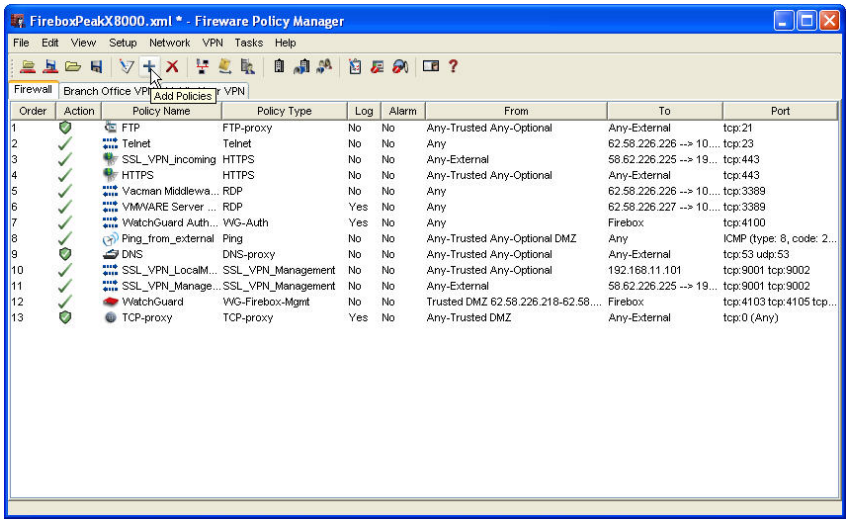

FireboxPeakX8000.xml * - Fireware Policy Manager
File Edit View Setup Network VPN Tasks Help
Add Policies
Firewall
Order Action Policy Name Policy Type Log Alarm From To Port
1 FTP FTP-proxy No No Any-Trusted Any-Optional Any-External tcp:21
2 Telnet Telnet No No Any 62.58.226.226 --> 10.... tcp:23
3 SSL_VPN_incoming HTTPS No No Any-External 58.62.226.225 --> 19... tcp:443
4 HTTPS HTTPS No No Any-Trusted Any-Optional Any-External tcp:443
5 Vacman Middlewa... RDP No No Any 62.58.226.226 --> 10.... tcp:3389
6 VMWARE Server ... RDP Yes No Any 62.58.226.227 --> 10.... tcp:3389
7 WatchGuard Auth... WG-Auth Yes No Any Firebox tcp:4100
8 Ping_from_external Ping No No Any-Trusted Any-Optional DMZ Any ICMP (type: 8, code: 2...
9 DNS DNS-proxy No No Any-Trusted Any-Optional Any-External tcp:53 udp:53
10 SSL_VPN_LocalM... SSL_VPN_Management No No Any-Trusted Any-Optional 192.168.11.101 tcp:9001 tcp:9002
11 SSL_VPN_Manage... SSL_VPN_Management No No Any-External 58.62.226.225 --> 19... tcp:9001 tcp:9002
12 WatchGuard WG-Firebox-Mgmt No No Trusted DMZ 62.58.226.218-62.58.... Firebox tcp:4103 tcp:4105 tcp...
13 TCP-proxy TCP-proxy Yes No Any-Trusted DMZ Any-External tcp:0 (Any)

Figure 13: Website Proxy Policy (1)

Select **HTTP-proxy** under the proxies folder and click **Add...** to continue.

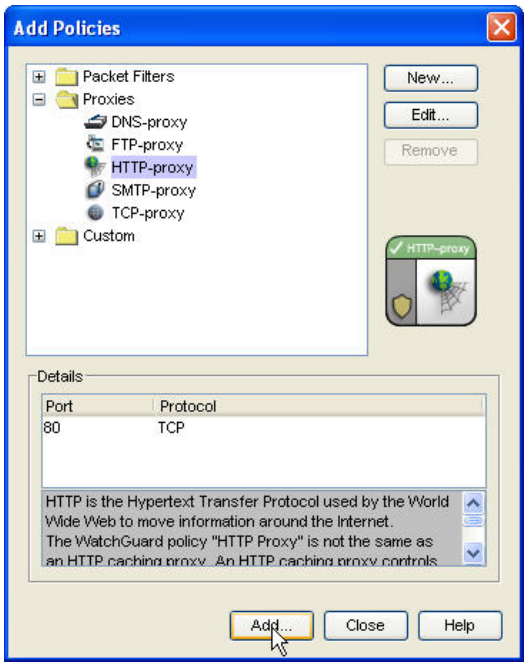


Figure 14: Website Proxy Policy (2)

Click the **Add...** button below the *From:* field to add a new allowed source.

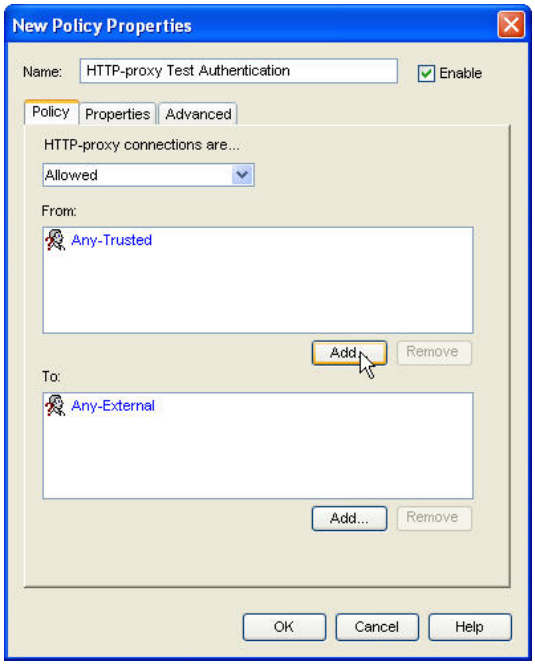


Figure 15: Website Proxy Policy (3)

Click the **Add User…** button.

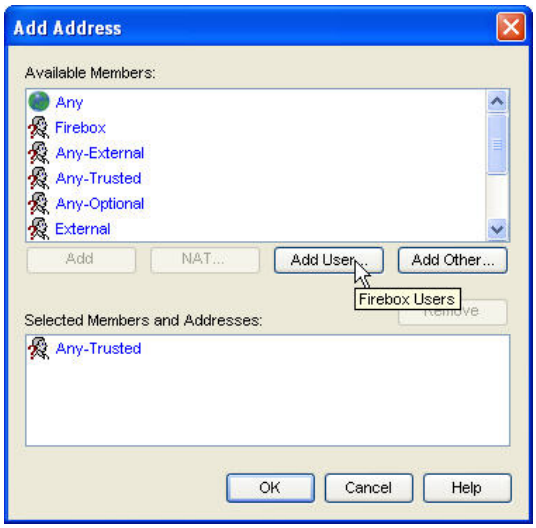


Figure 16: Website Proxy Policy (4)

Select **Firewall** as Type and **RADIUS** as Auth. Server. Make sure you type in the username as it is known in the back-end authentication service (Active Directory, VACMAN Middleware, …). Click **OK** to finish.

Figure 17: Website Proxy Policy (5)

Make sure you remove all unnecessary members and addresses from list. So you only keep a list of people who are allowed to access the corporate website.

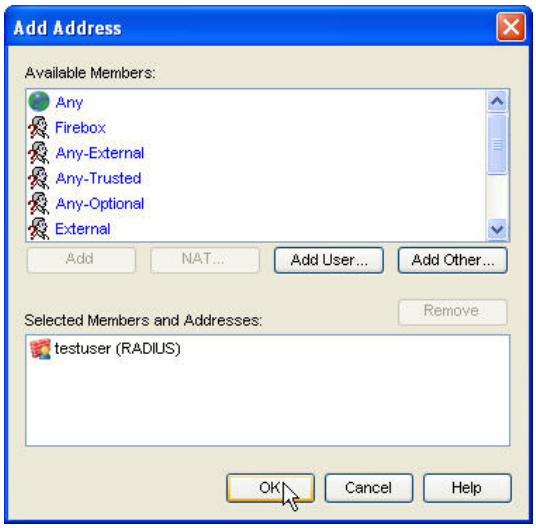


Figure 18: Website Proxy Policy (6)

*Note: It might be a though job to add a lot of users this way. This job can also be done by manually editing the configuration *.xml file.*

Click the **Add…** button below the *To:* field to configure the internal website that has to be protected.

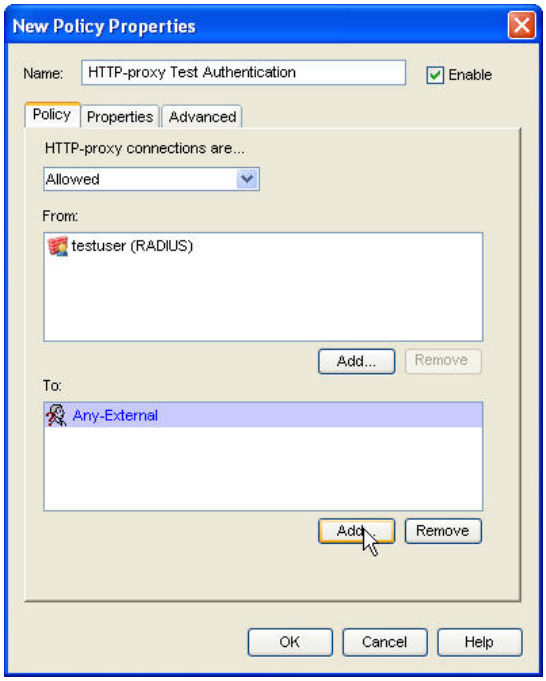


Figure 19: Website Proxy Policy (7)

Click the **NAT…** button to add a new link to an internal website.

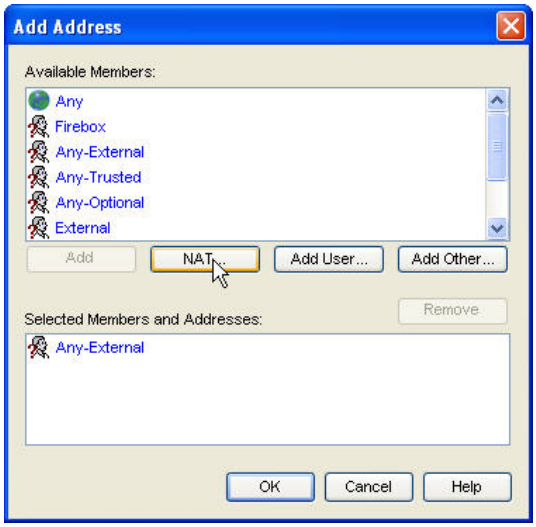


Figure 20: Website Proxy Policy (8)

If you have more then one IP Address pointing to the Firebox, you will have a choice of which **External IP Address** to use for the connection to the website. Also add the **Internal IP Address** of the web server hosting your corporate website. Click **OK** to finish.

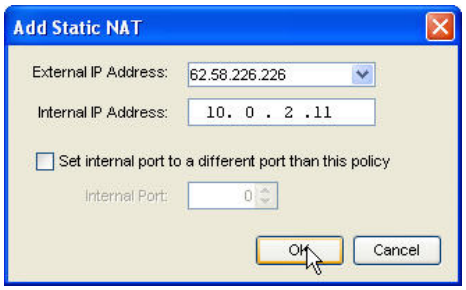


Figure 21: Website Proxy Policy (9)

If you have chosen NAT as *To:* address, all other fields are automatically removed from the list. You should only have kept the NAT address in the list.

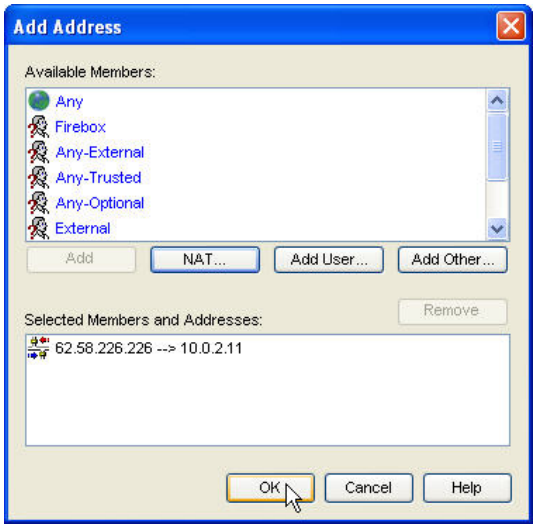


Figure 22: Website Proxy Policy (10)

The next screen gives you an overview of the changes made. We only **allow** some **authenticated users** to use a **NAT mapping** to the corporate website. Click **OK** to finish.

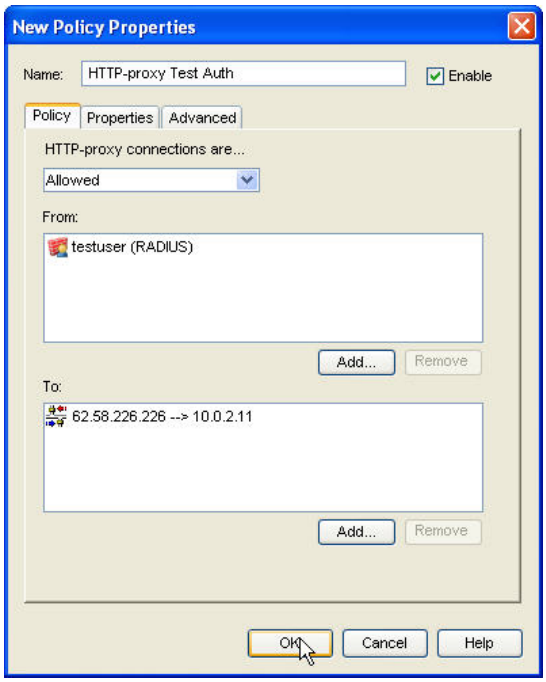


Figure 23: Website Proxy Policy (11)

Click the Close button in the Add Policies window to get back to the overview window. Here your newly created rule now should show up.

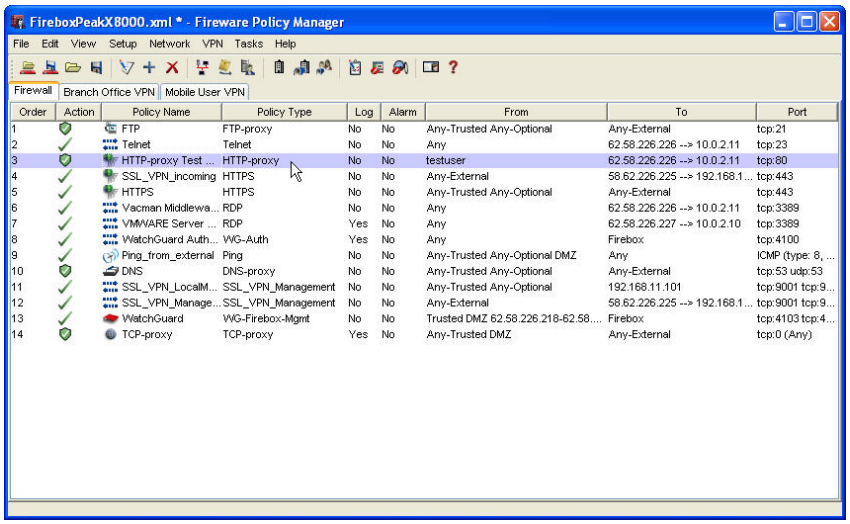
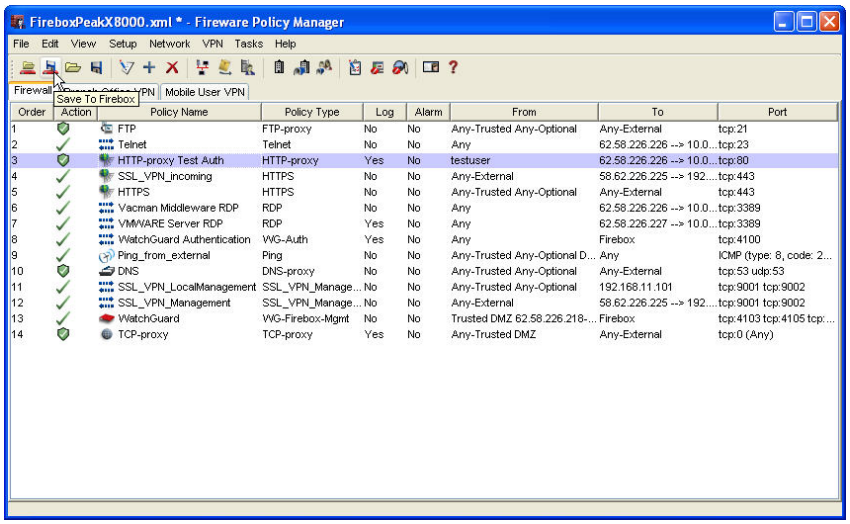

FireboxPeakX8000.xml * - Fireware Policy Manager
File Edit View Setup Network VPN Tasks Help
Firewall
Branch Office VPN
Mobile User VPN
Order Action Policy Name Policy Type Log Alarm From To Port
1 FTP FTP-proxy No No Any-Trusted Any-Optional Any-External tcp:21
2 Telnet Telnet No No Any 62.58.226.226 --> 10.0.2.11 tcp:23
3 HTTP-proxy Test ... HTTP-proxy No No testuser 62.58.226.226 --> 10.0.2.11 tcp:80
4 SSL_VPN_incoming HTTPS No No Any-External 58.62.226.225 --> 192.168.1... tcp:443
5 HTTPS HTTPS No No Any-Trusted Any-Optional Any-External tcp:443
6 Vacman Middlewa... RDP No No Any 62.58.226.226 --> 10.0.2.11 tcp:3389
7 VMWARE Server ... RDP Yes No Any 62.58.226.227 --> 10.0.2.10 tcp:3389
8 WatchGuard Auth... WG-Auth Yes No Any Firebox tcp:4100
9 Ping_from_external Ping No No Any-Trusted Any-Optional DMZ Any ICMP (type: 8, ...
10 DNS DNS-proxy No No Any-Trusted Any-Optional Any-External tcp:53 udp:53
11 SSL_VPN_LocalM... SSL_VPN_Management No No Any-Trusted Any-Optional 192.168.11.101 tcp:9001 tcp:9...
12 SSL_VPN_Manage... SSL_VPN_Management No No Any-External 58.62.226.225 --> 192.168.1... tcp:9001 tcp:9...
13 WatchGuard WG-Firebox-Mgmt No No Trusted DMZ 62.58.226.218-62.58.... Firebox tcp:4103 tcp:4...
14 TCP-proxy TCP-proxy Yes No Any-Trusted DMZ Any-External tcp:0 (Any)

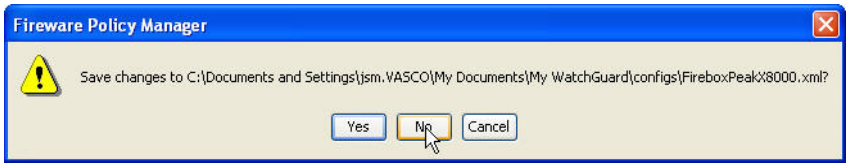
Figure 24: Website Proxy Policy (12)

5.5 Saving Changes

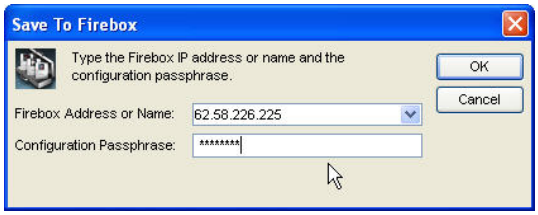
When all changes are performed, you must save the current configuration back to the Firebox. This is done by clicking the **Save To Firebox** button.


FireboxPeakX8000.xml * - Fireware Policy Manager
File Edit View Setup Network VPN Tasks Help
Save To Firebox
Mobile User VPN
Order Action Policy Name Policy Type Log Alarm From To Port
1 FTP FTP-proxy No No Any-Trusted Any-Optional Any-External tcp:21
2 Telnet Telnet No No Any 62.58.226.226 --> 10.0... tcp:23
3 HTTP-proxy Test Auth HTTP-proxy Yes No testuser 62.58.226.226 --> 10.0... tcp:80
4 SSL_VPN_incoming HTTPS No No Any-External 58.62.226.225 --> 192.... tcp:443
5 HTTPS HTTPS No No Any-Trusted Any-Optional Any-External tcp:443
6 Vacman Middleware RDP RDP No No Any 62.58.226.226 --> 10.0... tcp:3389
7 VMWARE Server RDP RDP Yes No Any 62.58.226.227 --> 10.0... tcp:3389
8 WatchGuard Authentication WG-Auth Yes No Any Firebox tcp:4100
9 Ping_from_external Ping No No Any-Trusted Any-Optional D... Any ICMP (type: 8, code: 2...
10 DNS DNS-proxy No No Any-Trusted Any-Optional Any-External tcp:53 udp:53
11 SSL_VPN_LocalManagement SSL_VPN_Manage... No No Any-Trusted Any-Optional 192.168.11.101 tcp:9001 tcp:9002
12 SSL_VPN_Management SSL_VPN_Manage... No No Any-External 58.62.226.225 --> 192.... tcp:9001 tcp:9002
13 WatchGuard WG-Firebox-Mgmt No No Trusted DMZ 62.58.226.218-... Firebox tcp:4103 tcp:4105 tcp:...
14 TCP-proxy TCP-proxy Yes No Any-Trusted DMZ Any-External tcp:0 (Any)

The program will ask you to store the current configuration locally to an *.xml file. Answer with **Yes or No**, depending you want to save it or not.



Now your have to give the write/configuration passphrase. This passphrase enables you to save changes to the Firebox. When this is done, the current configuration will be live on the Firebox.



6 VACMAN Middleware

6.1 Configure VACMAN Middleware

Setting up the VM only requires you to set up a policy to go to the right back-end and to add an extra Radius component pointing to the Firebox.

To add a new policy, right-click Policies and choose **New Policy**.

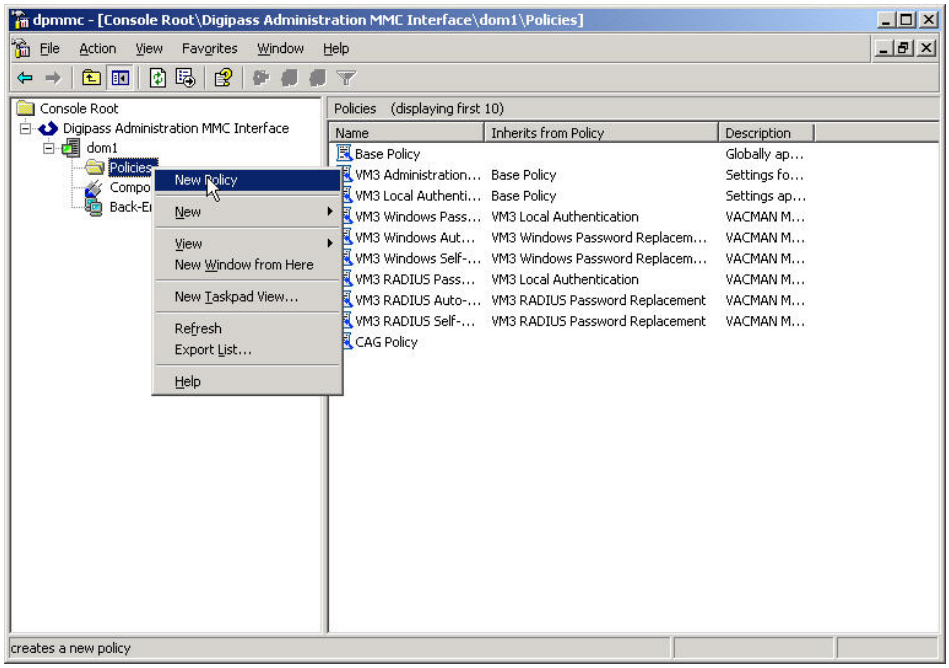


Figure 25: VM configuration (1)

There are a few policies available by default. You can also create new policies to suit your needs. Those can be independent policies or inherit their settings from default or other policies.

Fill in a **policy name** and choose the **option** most suitable in your situation. If you want the policy to inherit setting from another policy, choose the inherit option. If you want to copy an existing policy, choose the copy option and if you want to make a new one, choose the create option.

In our example we chose:
***Inherit** settings from **VM3 Windows Password Replacement**.*

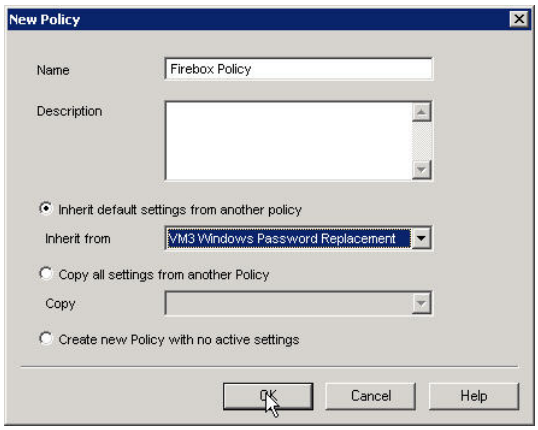


Figure 26: VM configuration (2)

In the policy options configure it to use the right back-end server. This could be the local database, but also active directory or another radius server.

This is probably the same that was in your Default Firebox authentication options before you changed it. Or you use the local database, Windows or you go further to another radius server.

In our example we select our newly made **Firebox Policy** and change it like this:

Main Settings
- *Local auth.:* Default (Digipass/Password)
- *Back-End Auth.:* **Always**
- *Back-End Protocol:* **RADIUS**

User Settings
- *Dynamic User Registration:* Default (Yes)
- *Password Autolearn:* Default (Yes)
- *Stored Password Proxy:* Default (Yes)
- *Windows Group Check:* **No Check**

Challenge Settings
- 2-Step Challenge Response **None**

After configuring this Policy, the authentication will happen in the back-end to a RADIUS proxy Server (IAS in this case). So user credentials are passed through to the VM, it will check these credentials with the IAS and will receive from IAS an Access-Accept or Access-Reject message. This message will be forwarded to the Firebox. At first we will use the “Response Only” method to authenticate.

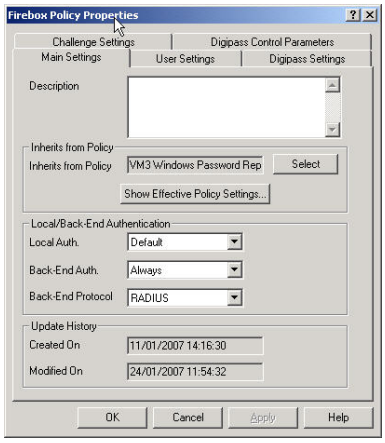


Figure 27: VM configuration (3)

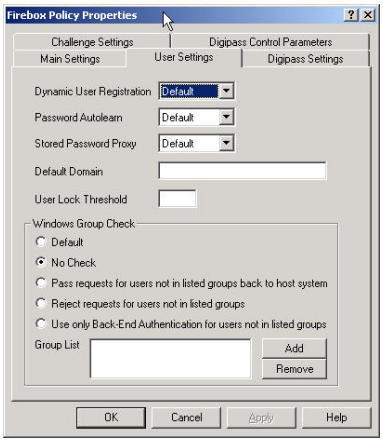


Figure 28: VM configuration (4)

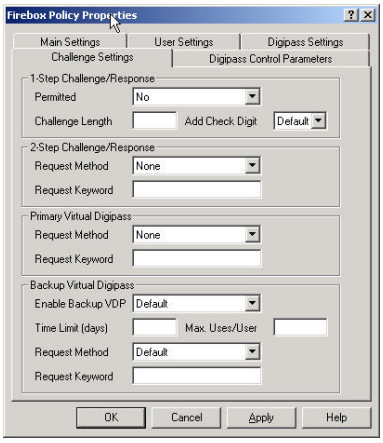


Figure 29: VM configuration (5)

Now create a new component by right-clicking the Components and choose **New Component**.

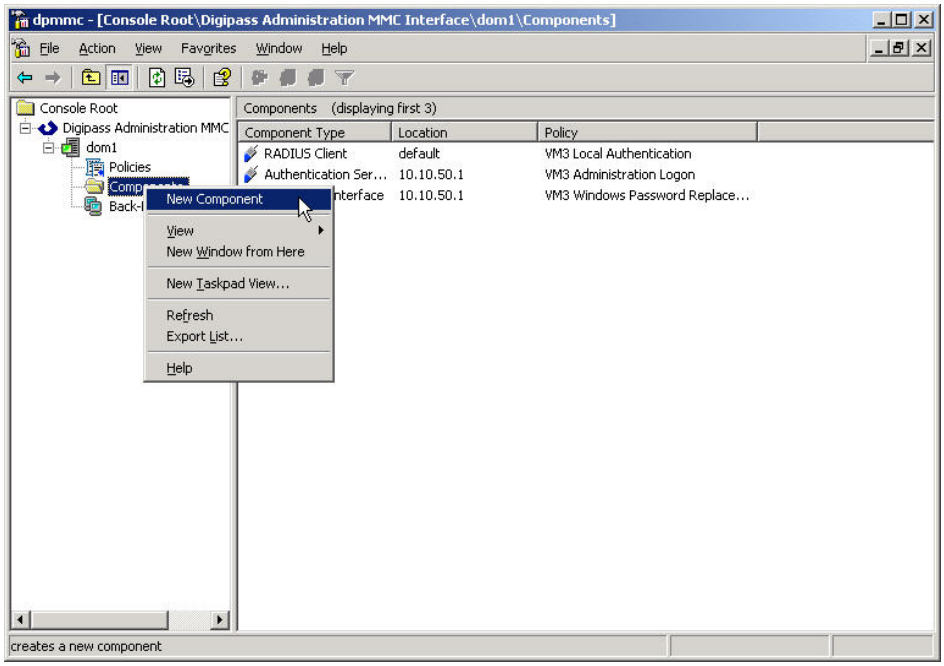


Figure 30: VM configuration (5)

As component type choose **RADIUS Client**. The location is the **IP address of the Firebox**. In the policy field you should find your **newly created policy**. Fill in the **shared secret** you entered also in the Firebox in the RADIUS options.

Click Create.

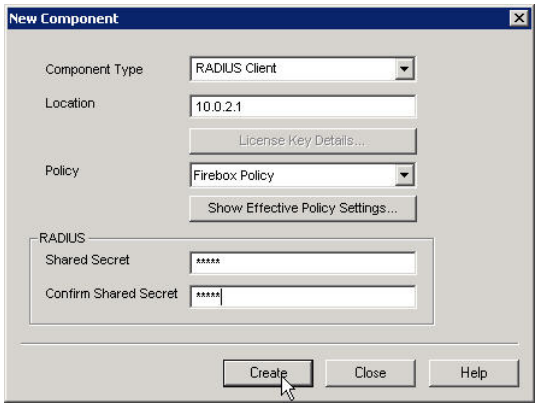


Figure 31: VM configuration (6)

As last we will add the back-end RADIUS authentication server settings.

Right-click Back-End Servers and select **New Back-End Server…**

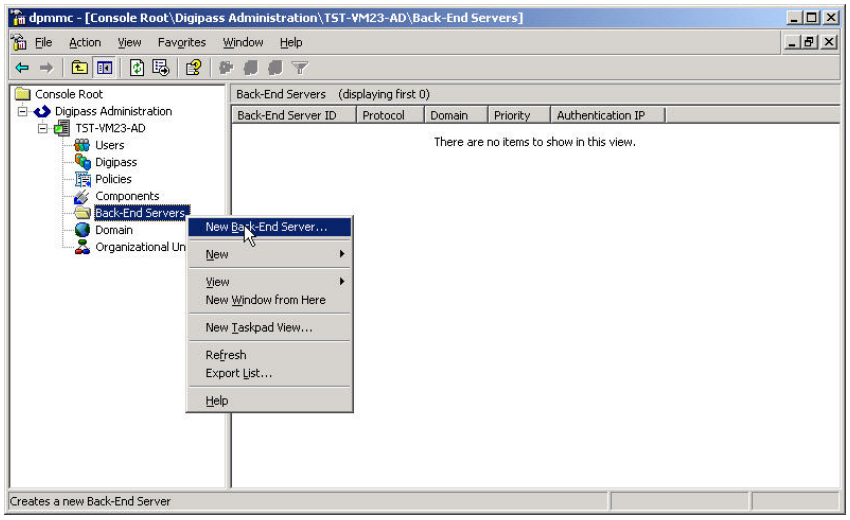
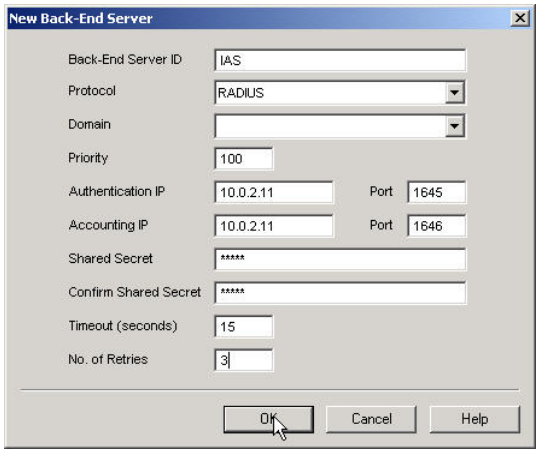


Figure 32: VM configuration (7)

Fill in all fields according to the server where IAS is configured.



Server ID:	Name of this element
Protocol:	RADIUS
Domain:	leave empty
Priority:	100
Auth. IP:	IAS Server + port
Acc. IP:	IAS Server + port
Secret:	the same as on IAS
Timeout:	15
Retries:	3

Figure 33: VM configuration (8)

The Firebox and the VM are set up. Now we will setup the back-end authentication service: IAS.

7 Microsoft IAS

In this chapter we will explain how to use IAS as a back-end authentication server. The reason for doing this is because in IAS we can do an AD Group check. We will setup IAS to check if the users are in a certain AD group. If they are, we will send a group string back in the Filter-Id attribute, which is an attribute of the standard RADIUS message.

Open the IAS administration window, right-click RADIUS Clients and select **New RADIUS Client**.

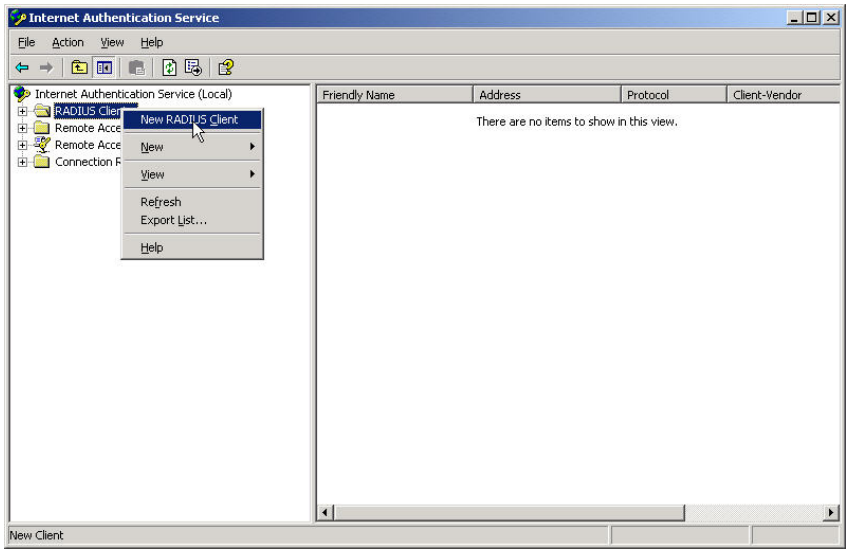


Figure 34: IAS configuration (1)

Fill in a **name** and the **IP address or hostname** of the server where VACMAN Middleware is installed. Click **Next** to continue.

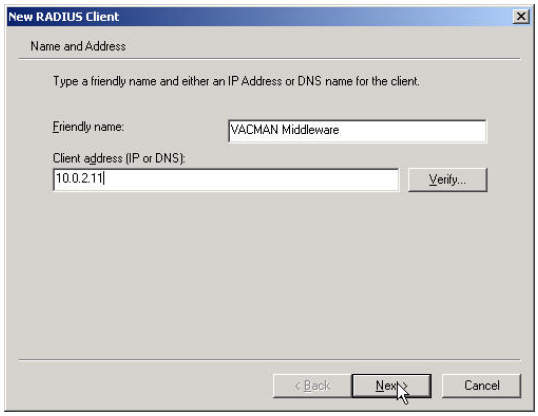


Figure 35: IAS configuration (2)

There are no vendor specific attributes we need for this message, so select **RADIUS Standard** as client vendor. Type in the same **Shared Secret** as you entered in the Back-End authentication server in VACMAN Middleware.

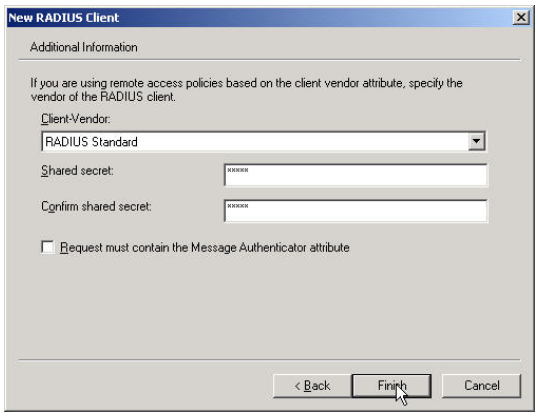

New RADIUS Client
Additional Information
If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.
Client-Vendor:
RADIUS Standard
Shared secret:
Confirm shared secret:
Request must contain the Message Authenticator attribute
< Back
Finish
Cancel

Figure 36: IAS configuration (3)

To create the policy that will check for user groups, go to Remote Access Policies, right-click this folder and select **New Remote Access Policy**.

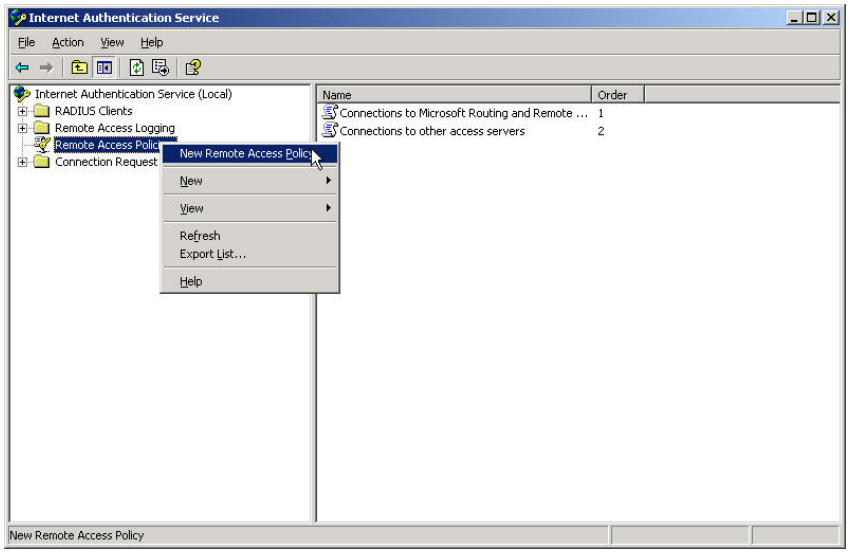


Figure 37: IAS configuration (4)

Select to **Set up a custom policy** and type in a friendly name for this policy. As you may want to check different groups, it could be appropriate to reference the name of the group in your friendly name. For each group you will need a different policy.

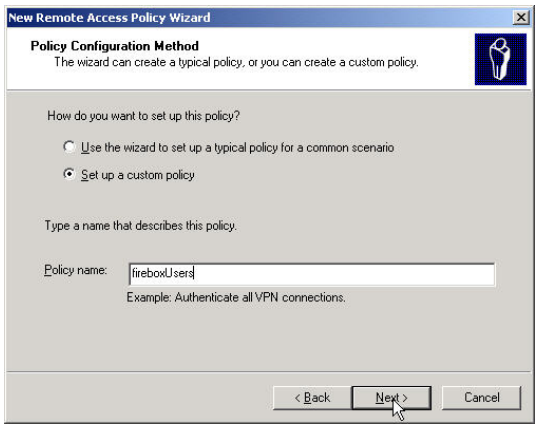

New Remote Access Policy Wizard
Policy Configuration Method
The wizard can create a typical policy, or you can create a custom policy.
How do you want to set up this policy?
Use the wizard to set up a typical policy for a common scenario
Set up a custom policy
Type a name that describes this policy.
Policy name:
fireboxUsers
Example: Authenticate all VPN connections.
< Back
Next >
Cancel

Figure 38: IAS configuration (5)

Next, you are able to set the policy conditions. These conditions will have to be fulfilled before an authentication can be done. So here we will specify the group the user will have to belong to. Click the **Add…** button.

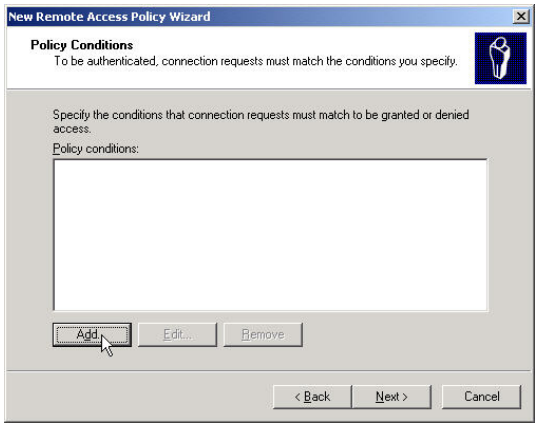

New Remote Access Policy Wizard
Policy Conditions
To be authenticated, connection requests must match the conditions you specify.
Specify the conditions that connection requests must match to be granted or denied access.
Policy conditions:
Add...
Edit...
Remove
< Back
Next >
Cancel

Figure 39: IAS configuration (6)

Select **Windows Groups** from the list and click **Add…**

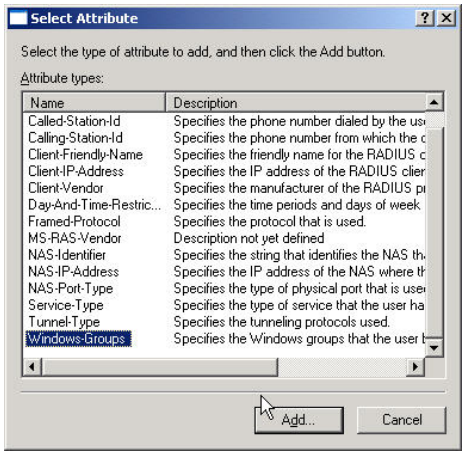


Figure 40: IAS configuration (7)

Click the **Add...** button to add an AD group to the list.

Figure 41: IAS configuration (8)

Search for the group the user has to belong to and click **OK**.

In our example we use the firebox_users group.

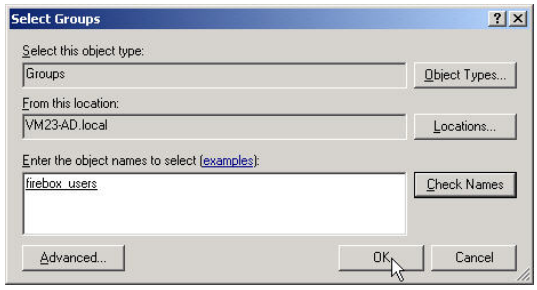


Figure 42: IAS configuration (9)

Click **OK** when the group shows up in the list.

Figure 43: IAS configuration (10)

Click **Next** to continue the wizard.

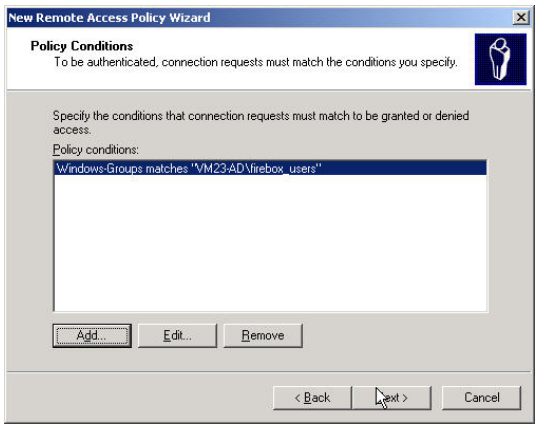

New Remote Access Policy Wizard
Policy Conditions
To be authenticated, connection requests must match the conditions you specify.
Specify the conditions that connection requests must match to be granted or denied access.
Policy conditions:
Windows-Groups matches "VM23-AD\firebox_users"
Add...
Edit...
Remove
< Back
Next >
Cancel

Figure 44: IAS configuration (11)

Select the **Grant remote access permission** and click **Next**.

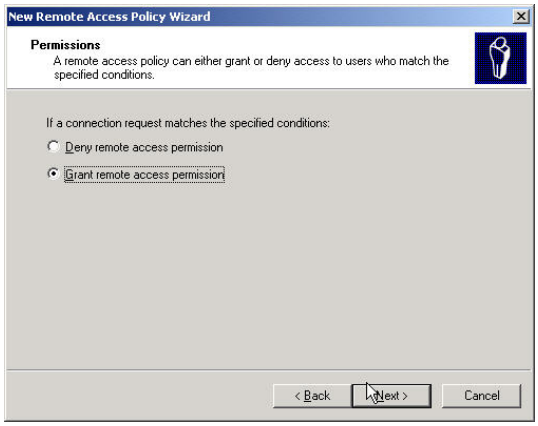

New Remote Access Policy Wizard
Permissions
A remote access policy can either grant or deny access to users who match the specified conditions.
If a connection request matches the specified conditions:
Deny remote access permission
Grant remote access permission
< Back
Next >
Cancel

Figure 45: IAS configuration (12)

This far the policy is set up. But we also wanted to send a group name back to the Firebox. Click **Edit Profile…**

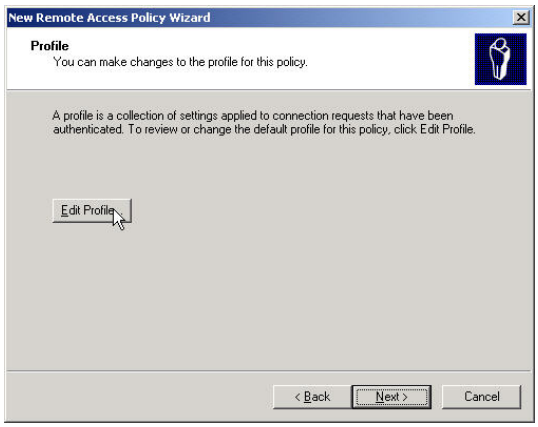

New Remote Access Policy Wizard
Profile
You can make changes to the profile for this policy.
A profile is a collection of settings applied to connection requests that have been authenticated. To review or change the default profile for this policy, click Edit Profile.
Edit Profile...
< Back
Next >
Cancel

Figure 46: IAS configuration (13)

Go to the **Authentication tab** and select **Unencrypted authentication (PAP, SPAP)** in the list.

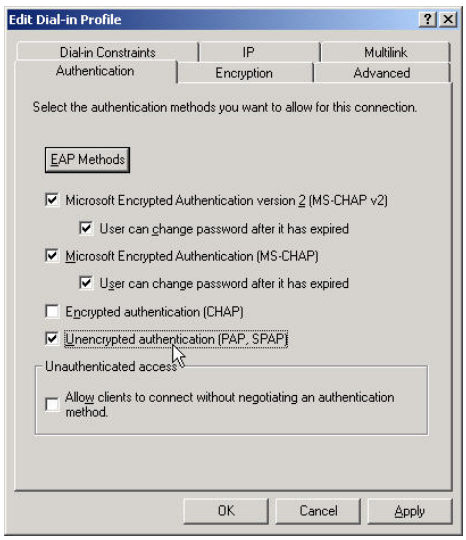


Figure 47: IAS configuration (14)

On the **Advanced tab**, click the **Add...** button.

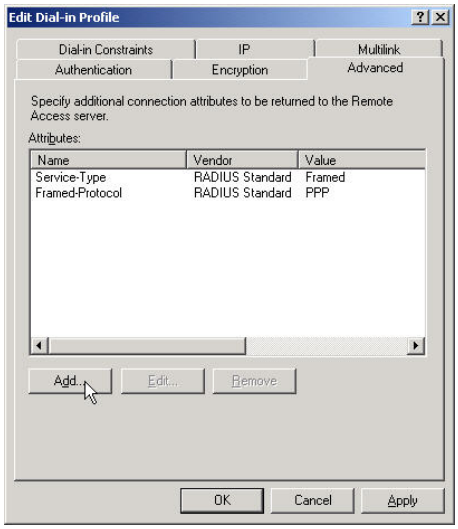


Figure 48: IAS configuration (15)

Select **Filter-Id** from the list and click **Add…**

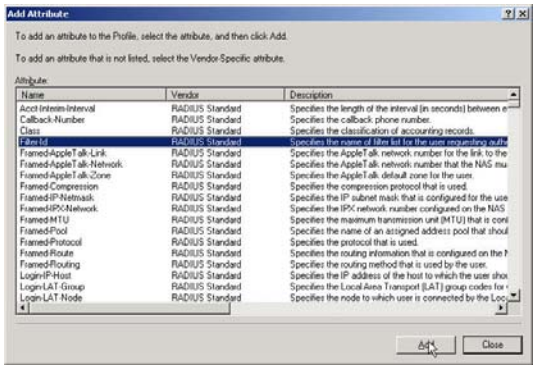


Figure 49: IAS configuration (16)

Click **Add…** to enter a new filter string.

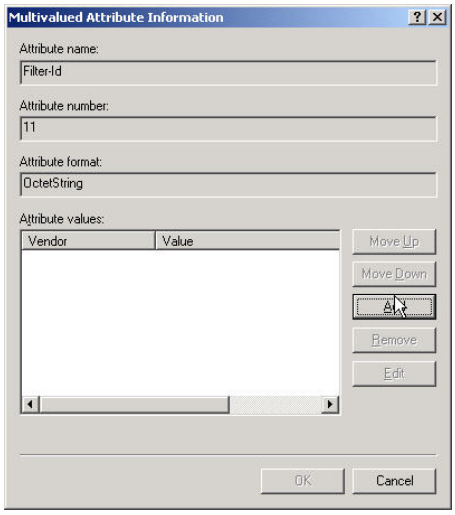


Figure 50: IAS configuration (17)

Make sure **String** is selected and enter the **group name** as you used it on the Firebox. The group name you enter here and like it is used in AD does not have to match. Click **OK** to go on.

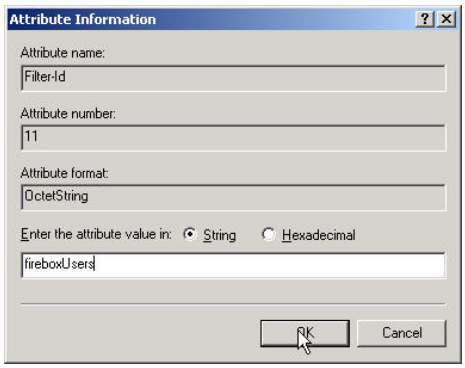


Figure 51: IAS configuration (18)

Click **OK** when the group name is shown in the attribute list.

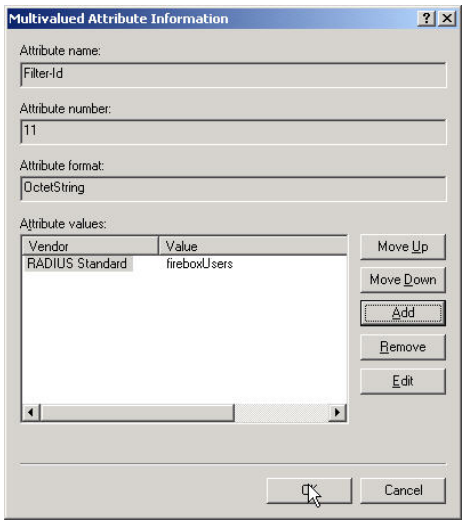


Figure 52: IAS configuration (19)

Click **Close** to go back.

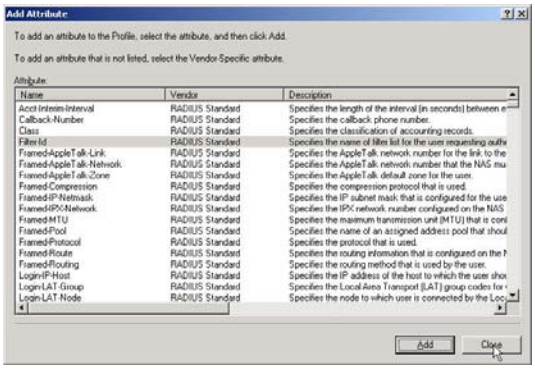


Figure 53: IAS configuration (20)

Click **OK** to save the changes you made to the profile and to go back to the wizard.

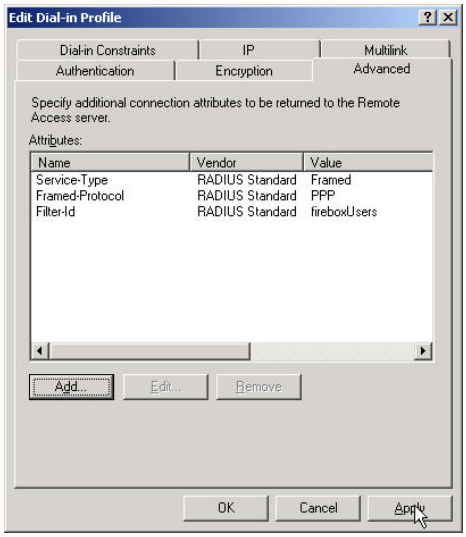


Figure 54: IAS configuration (21)

You will receive a warning stating you selected different authentication methods. Click **No** as we don't need to see additional help topics.

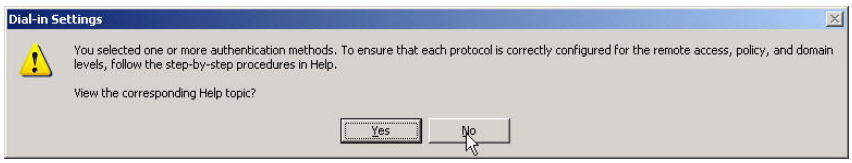

Dial-in Settings
You selected one or more authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.
View the corresponding Help topic?
Yes
No

Figure 55: IAS configuration (22)

Click **Next**.

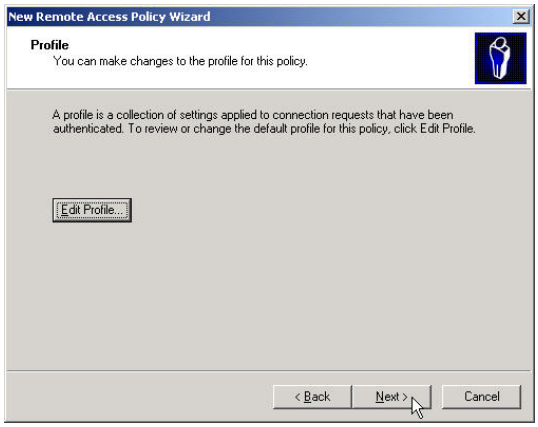

New Remote Access Policy Wizard
Profile
You can make changes to the profile for this policy.
A profile is a collection of settings applied to connection requests that have been authenticated. To review or change the default profile for this policy, click Edit Profile.
Edit Profile...
< Back
Next >
Cancel

Figure 56: IAS configuration (23)

The wizard is now complete and our policy is created. We will now be able to return a group object to the firebox. Click **Finish**.

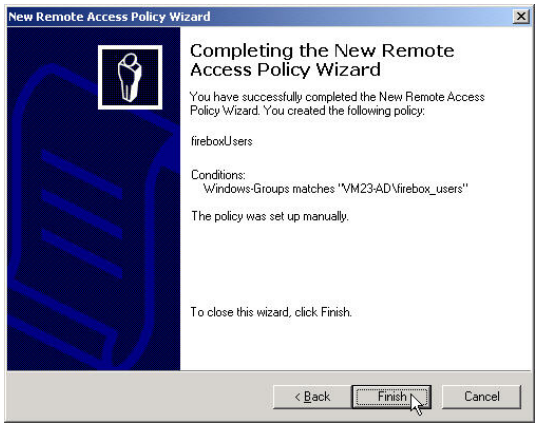

New Remote Access Policy Wizard
Completing the New Remote Access Policy Wizard
You have successfully completed the New Remote Access Policy Wizard. You created the following policy:
fireboxUsers
Conditions:
Windows-Groups matches "VM23-AD\firebox_users"
The policy was set up manually.
To close this wizard, click Finish.
< Back
Finish
Cancel

Figure 57: IAS configuration (24)

8 User configuration

The **user creation** steps you will find in this chapter are optional when you didn't activate the option **Dynamic User Registration (DUR) and/or Password Autolearn** in your policy settings.

The assignment of a DIGIPASS can happen manually as explained in the steps below. The user creation and DIGIPASS assignment steps depend on which database back-end you installed VACMAN Middleware. Either you installed it with an ODBC back-end or with an Active Directory back-end.

8.1 ODBC installation

8.1.1 User creation

User creation, while using an ODBC back-end, will happen in the DIGIPASS Administration MMC. Right-click the Users folder and select **New User ...**.

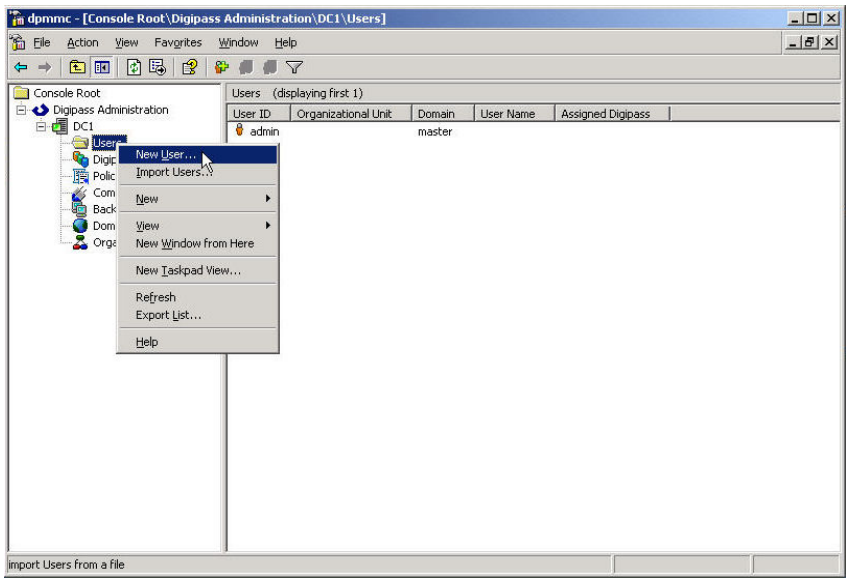


Figure 58: ODBC User Creation (1)

Fill in the username and password fields. Optionally choose the right domain and Organizational Unit and click the **Create** button.

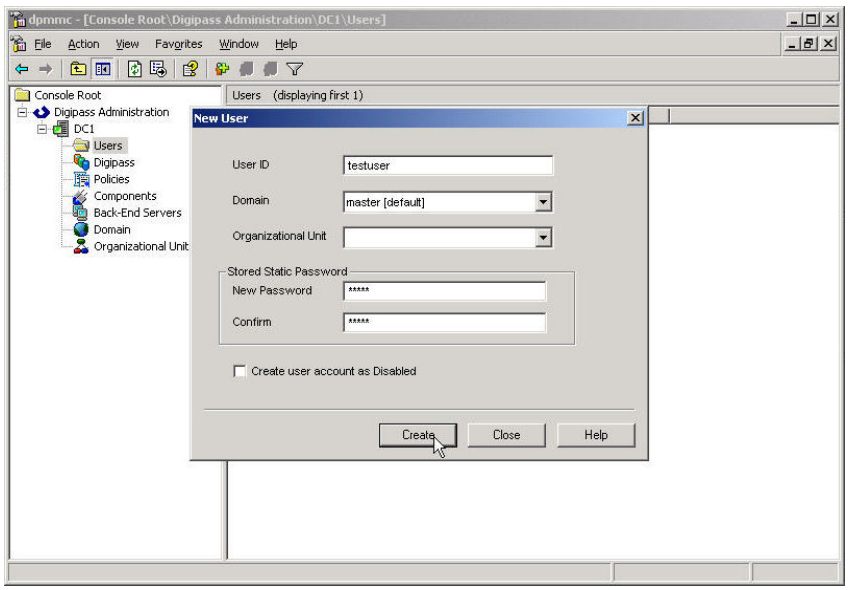


Figure 59: ODBC User Creation (2)

The user will now show up in the Users list of you DIGIPASS Administration MMC. At this point it will be exactly the same as when Dynamic User Recognition (DUR) was enabled.

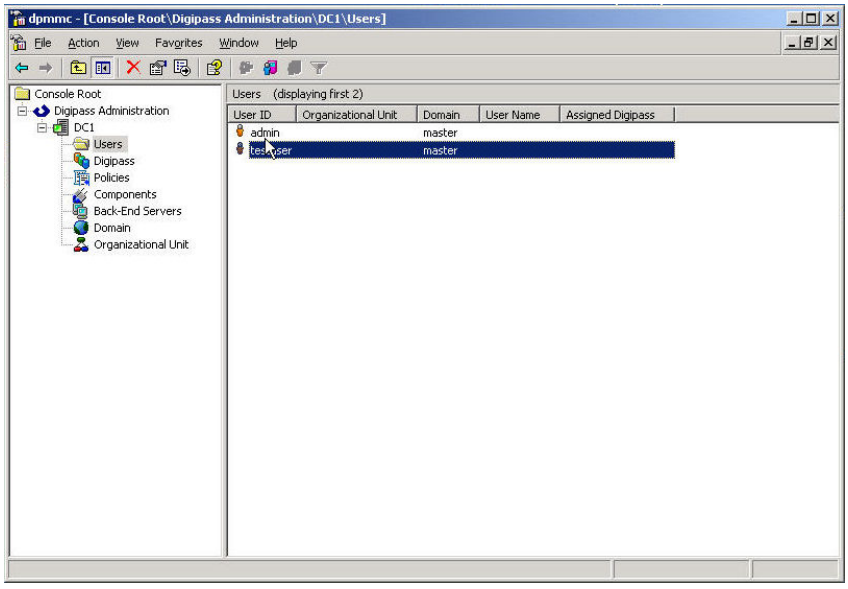


Figure 60: ODBC User Creation (3)

8.1.2 Import DIGIPASS

Right-click the DIGIPASS folder and select **Import DIGIPASS...** .

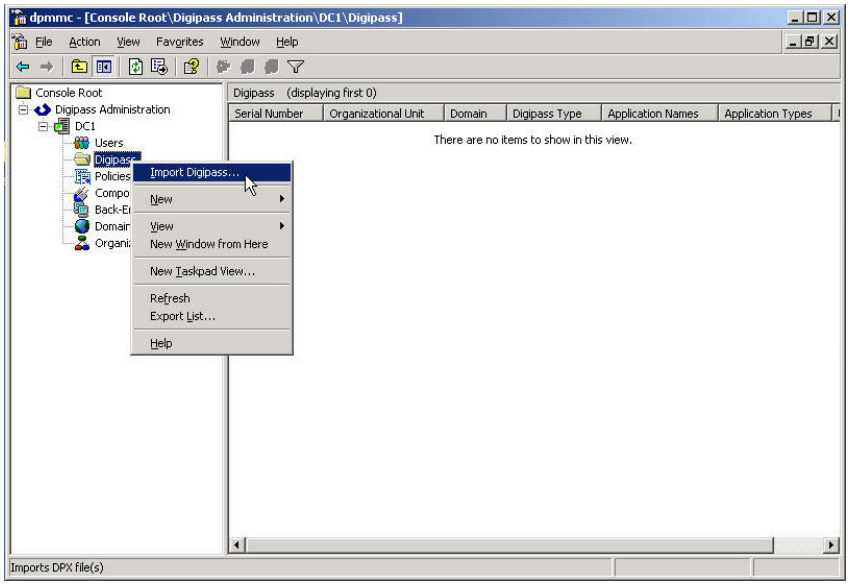


Figure 61: Import DIGIPASS (1)

Browse for your *.DPX file, fill in the Transport Key and look at your available applications by pushing the **Show Applications** button. You can either import all applications or only the ones you selected, by the **Import ...** buttons above and below the Show Applications button.

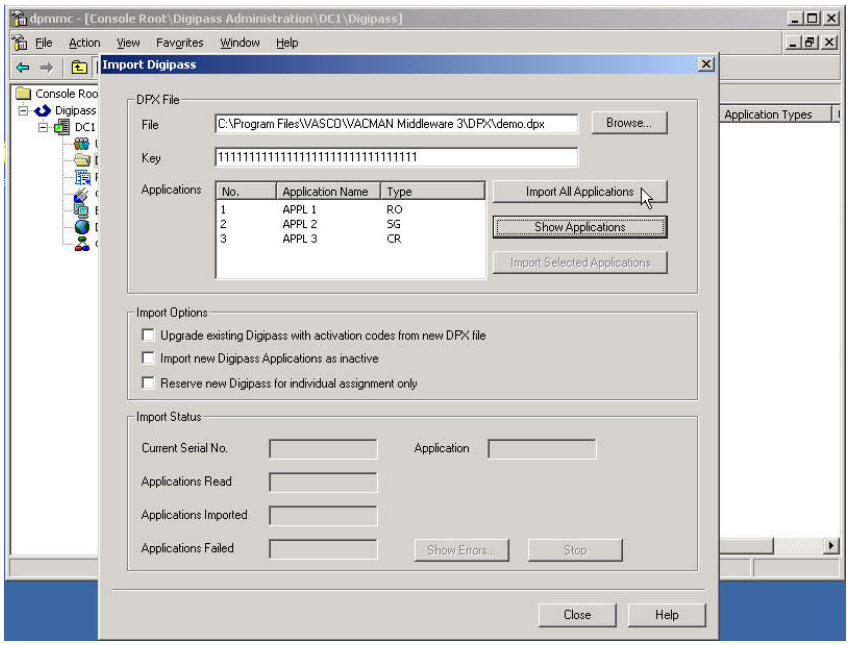


Figure 62: Import DIGIPASS (2)

When the DIGIPASS is imported successfully you will receive a confirmation message.

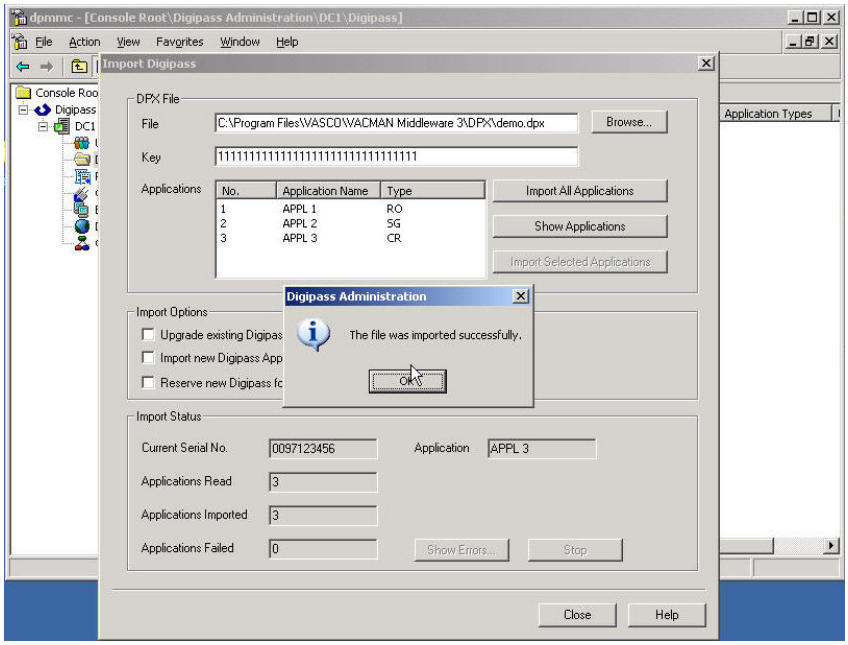


Figure 63: Import DIGIPASS (3)

8.1.3 DIGIPASS Assignment

There are two possible ways to assign a DIGIPASS to a user. You can search for a DIGIPASS and assign it to a user or you can search for a user and assign it to a DIGIPASS. You can see the difference in the following two figures.

Right-click a user and select **Assign DIGIPASS...** or …

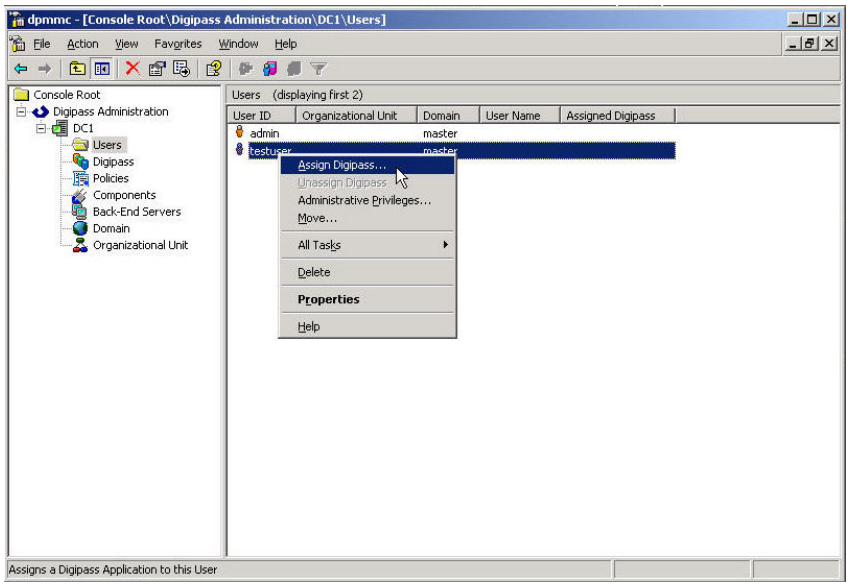


Figure 64: DIGIPASS assignment (1)

… you can right-click a DIGIPASS and select **Assign …** .

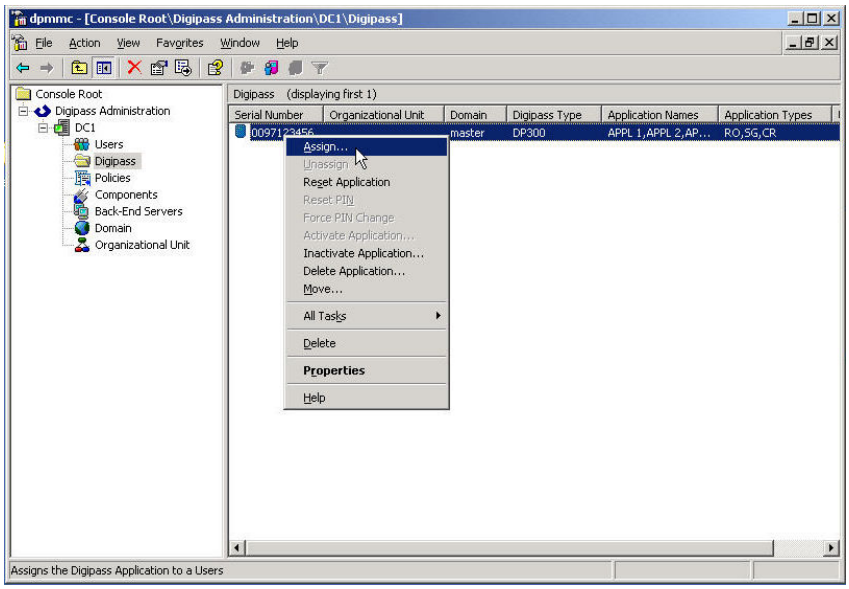


Figure 65: DIGIPASS assignment (2)

If you leave the User ID **blank** and press the **Find** button, you will get a list of all the available users in the same domain as the DIGIPASS. The usernames are partly searchable too.

Notice: If no users show up, make sure the domains of the DIGIPASS and the user match.

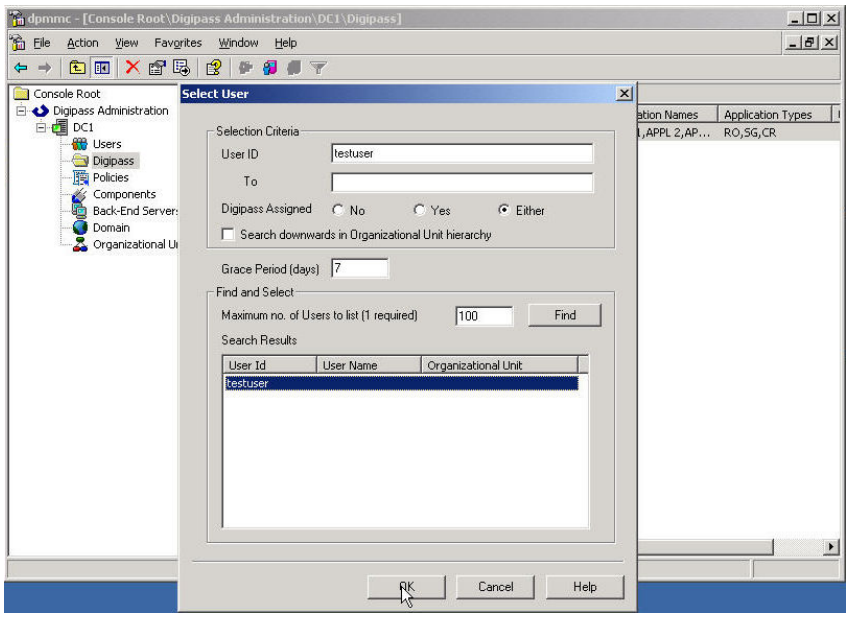


Figure 66: DIGIPASS assignment (3)

When assigning a DIGIPASS to a user the same procedure will be applicable. You can either select the desired option to search for a DIGIPASS or search through serial number. Leaving all options blank will show all possibilities in the same domain.

When the DIGIPASS gets successfully added to your user you will get a confirmation message.

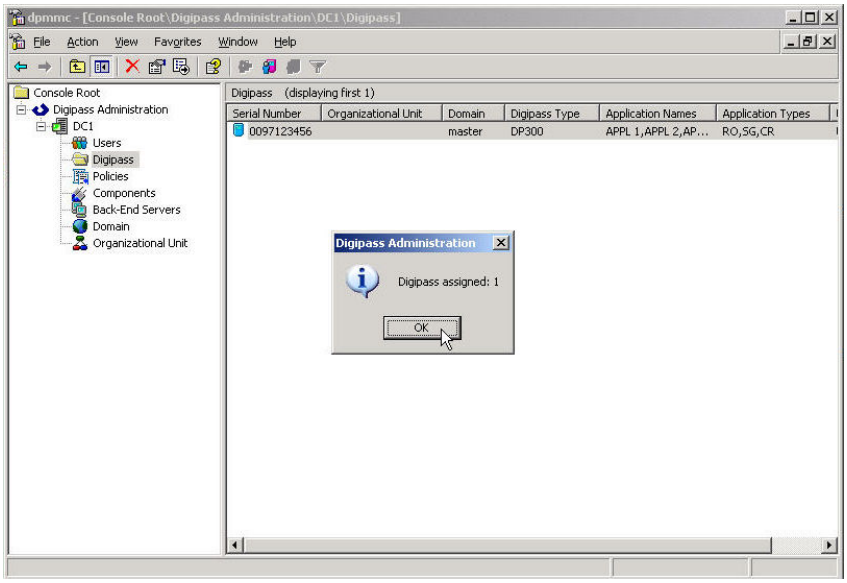


Figure 67: DIGIPASS assignment (4)

8.2 Active Directory installation

8.2.1 User creation

User creation, while using an Active Directory back-end, will happen in the **Active Directory Users and Computers MMC**. Right-click a user and select **Properties**. This can happen automatically when the Dynamic User Registration (DUR) option in the policy settings is active.

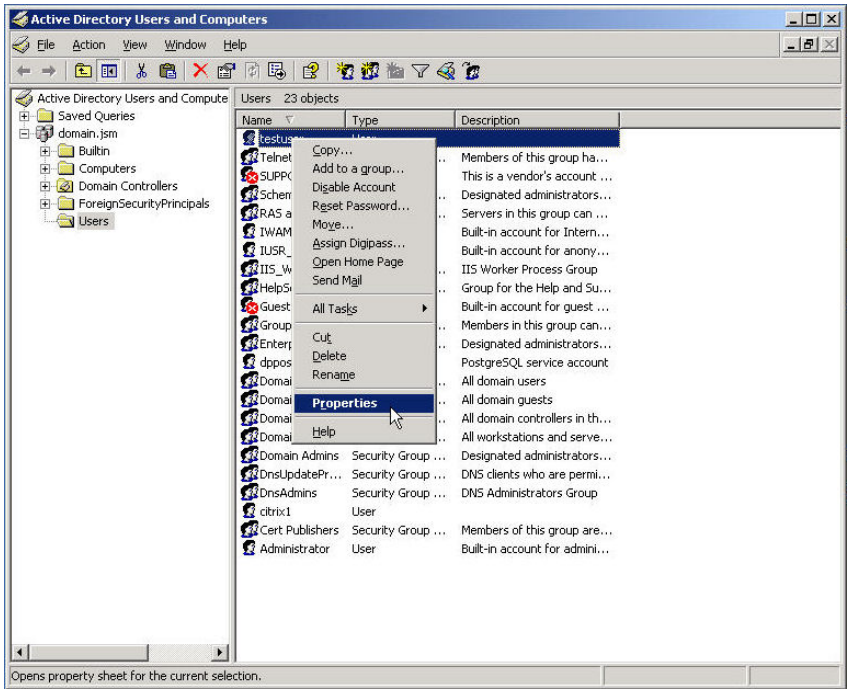


Figure 68: Active Directory User Creation (1)

In the **DIGIPASS User Account** tab you will see a field to manually add a password. This can also be automatically filled by enabling the Password Autolearn option in the policy settings.

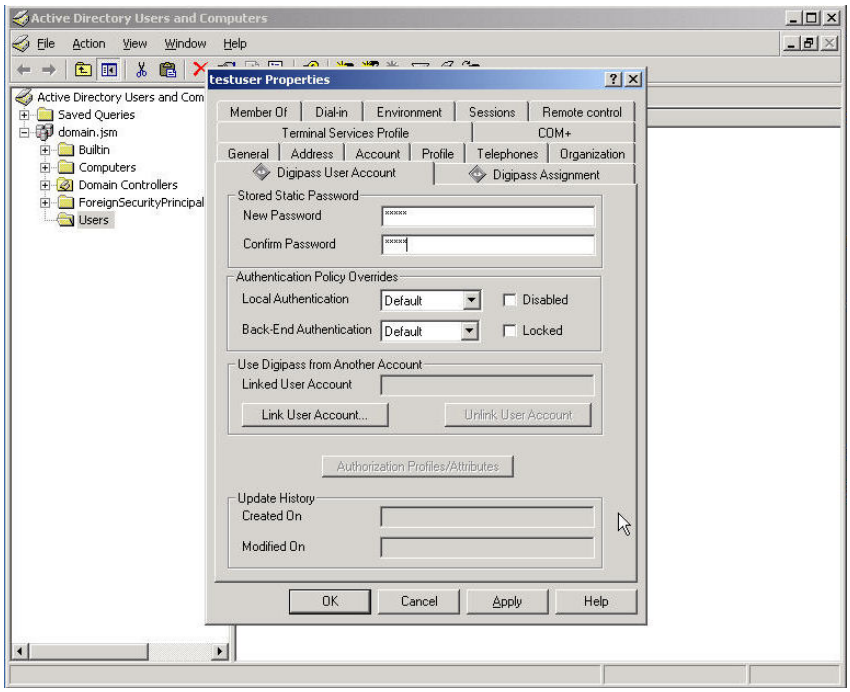


Figure 69: Active Directory User Creation (2)

After clicking the Apply button you will see the Update History fields being filled with the current date and time. When these fields are filled it means the DIGIPASS account exists and can be used.

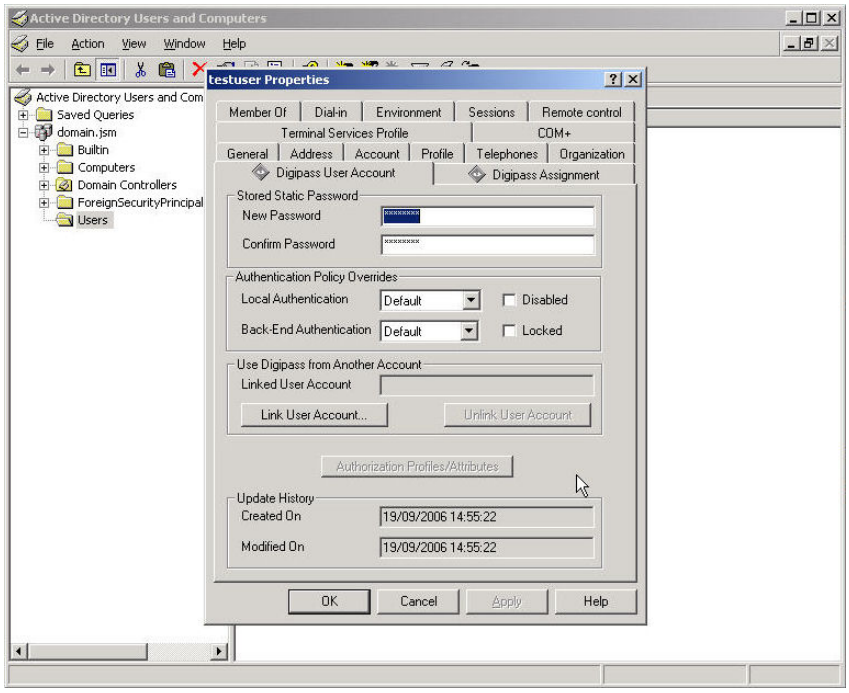


Figure 70: Active Directory User Creation (3)

8.2.2 Import DIGIPASS

To make sure you can see the DIGIPASS folders in the MMC, go to **View** and select the **Advanced Features**. This way you will see the DIGIPASS folders.

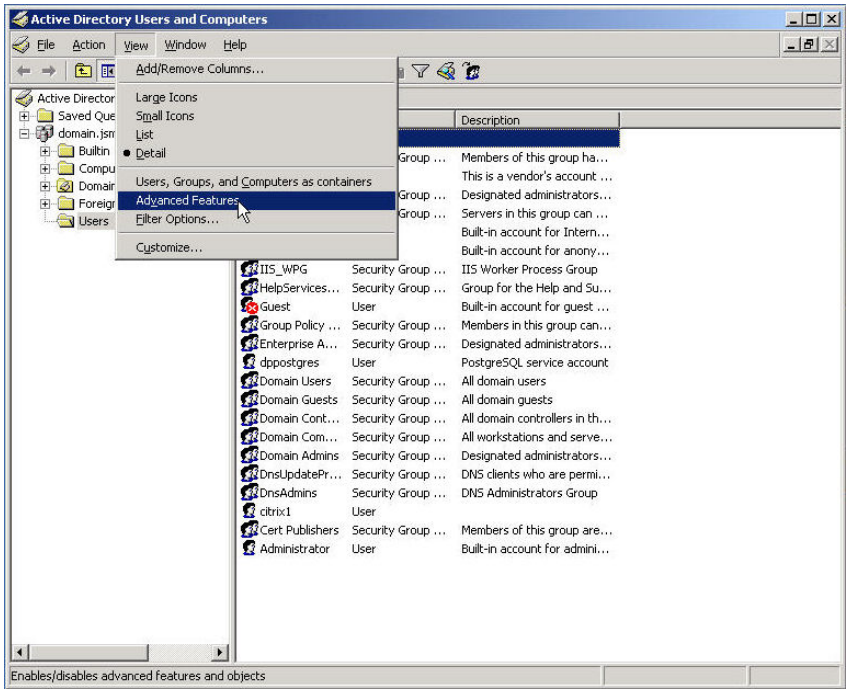

Active Directory Users and Computers
File Action View Window Help
Add/Remove Columns...
Large Icons
Small Icons
List
Detail
Users, Groups, and Computers as containers
Advanced Features
Filter Options...
Customize...
Description
Members of this group ha...
This is a vendor's account ...
Designated administrators...
Servers in this group can ...
Built-in account for Intern...
Built-in account for anony...
IIS_WPG Security Group ... IIS Worker Process Group
HelpServices... Security Group ... Group for the Help and Su...
Guest User Built-in account for guest ...
Group Policy ... Security Group ... Members in this group can...
Enterprise A... Security Group ... Designated administrators...
dppostgres User PostgreSQL service account
Domain Users Security Group ... All domain users
Domain Guests Security Group ... All domain guests
Domain Cont... Security Group ... All domain controllers in th...
Domain Com... Security Group ... All workstations and serve...
Domain Admins Security Group ... Designated administrators...
DnsUpdatePr... Security Group ... DNS clients who are permi...
DnsAdmins Security Group ... DNS Administrators Group
citrix1 User
Cert Publishers Security Group ... Members of this group are...
Administrator User Built-in account for admini...
Enables/disables advanced features and objects

Figure 71: Import DIGIPASS (1)

Right-click the **DIGIPASS-Pool** folder and select **Import DIGIPASS …** .

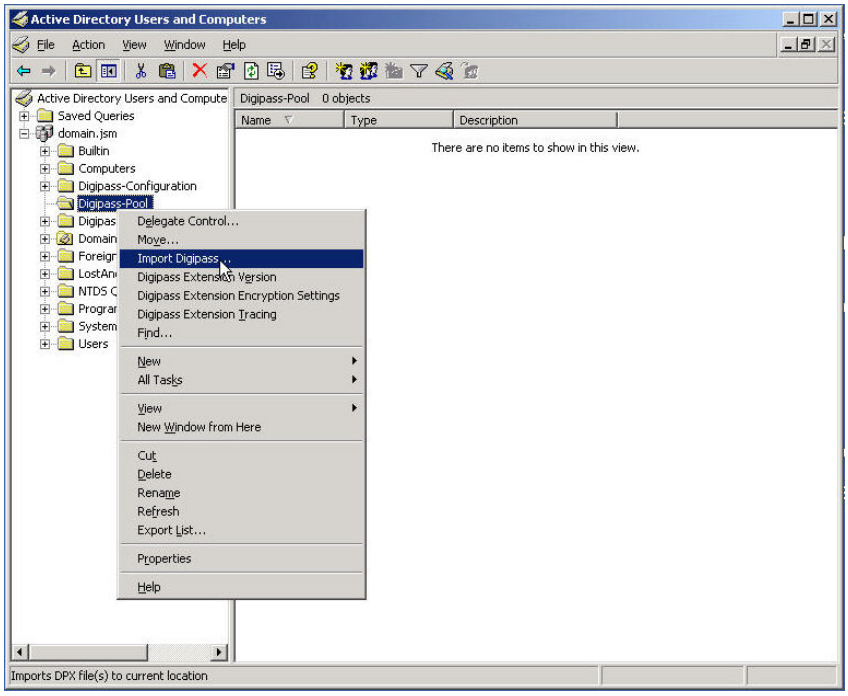


Figure 72: Import DIGIPASS (1)

Browse for your *.DPX file, fill in the Transport Key and look at your available applications by pushing the **Show Applications** button. You can either import all applications or only the ones you selected, by the **Import …** buttons above and below the Show Applications button.

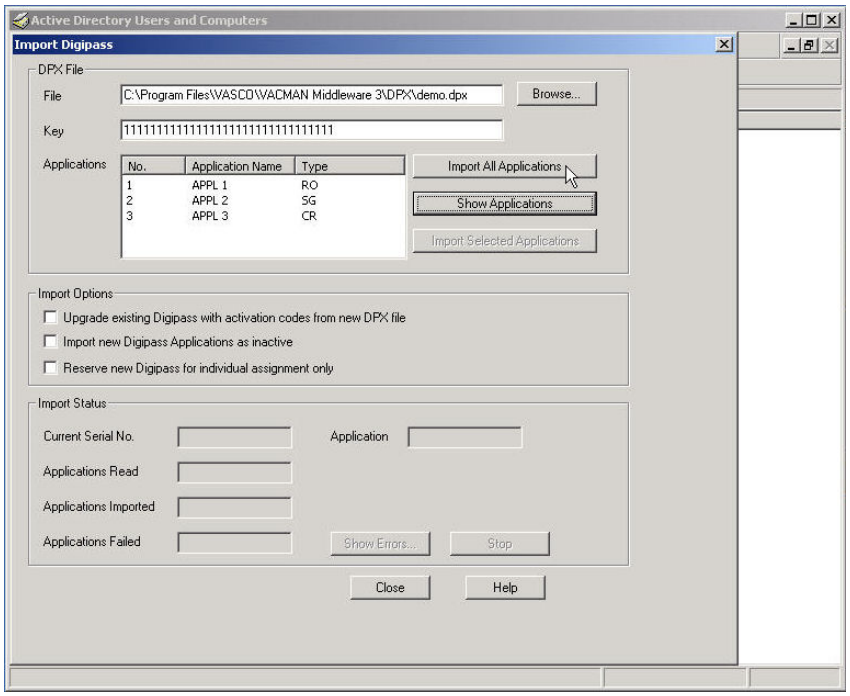


Figure 73: Import DIGIPASS (1)

When the DIGIPASS is imported successfully you will receive a confirmation message.

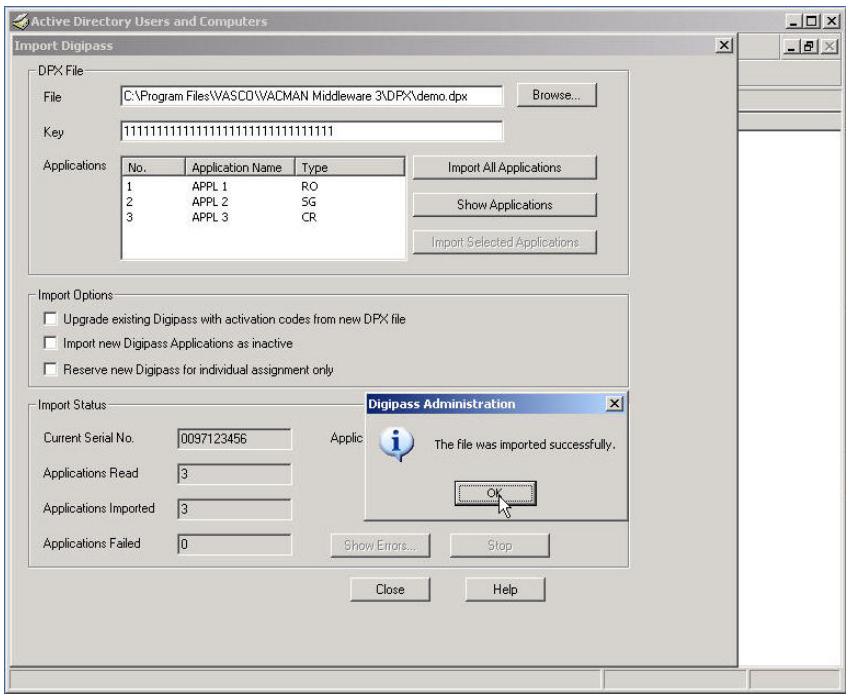


Figure 74: Import DIGIPASS (1)

8.2.3 DIGIPASS assignment

There are two possible ways to assign a user to a DIGIPASS. You can search for a DIGIPASS and assign it to a user or you can search for a user and assign it to a DIGIPASS. You can see the difference in the following two figures.

Right-click a **User** and select **Assign DIGIPASS...** or …

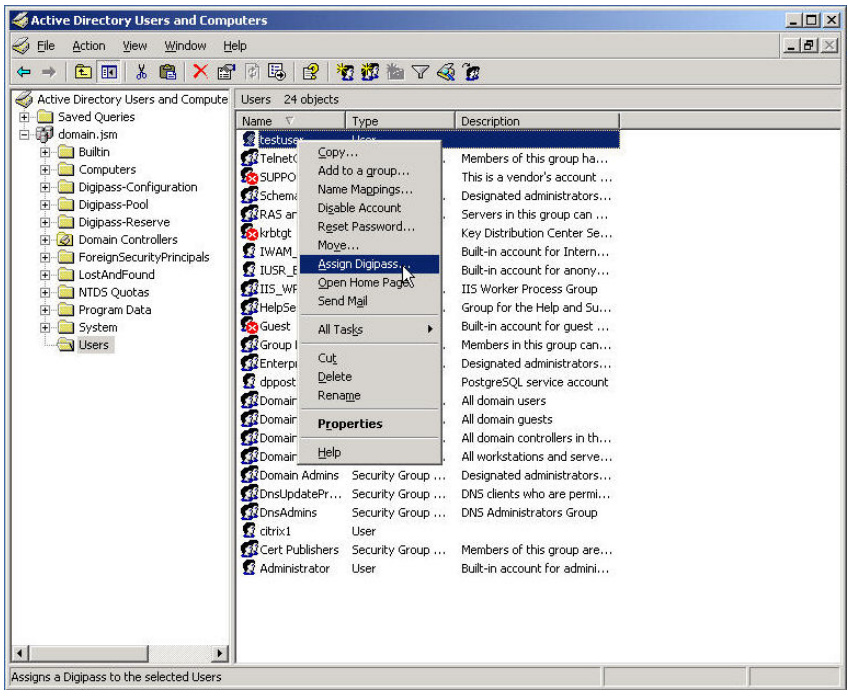


Figure 75: DIGIPASS Assignment (1)

… right-click a **DIGIPASS** and select **Assign DIGIPASS …** .

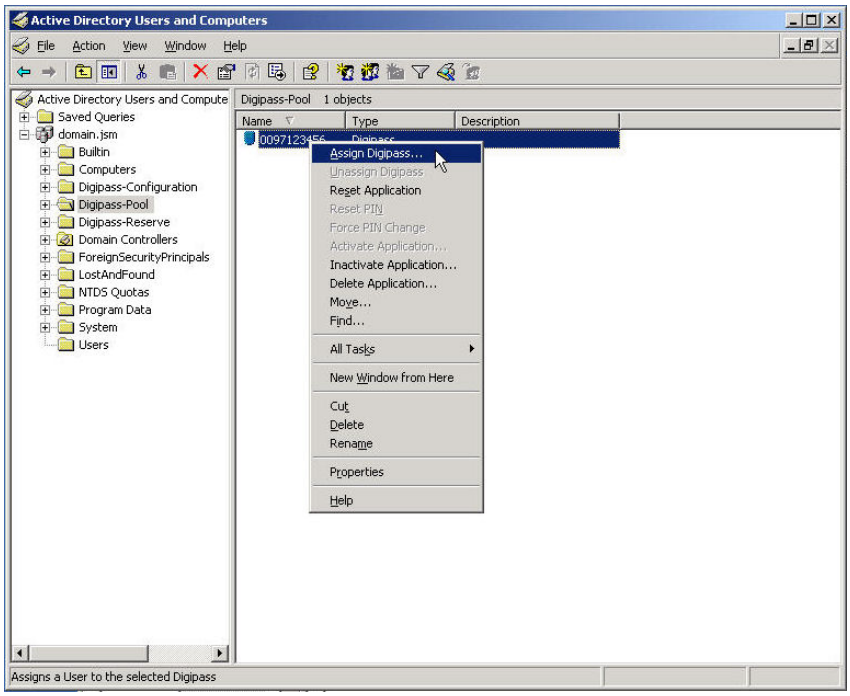


Figure 76: DIGIPASS Assignment (2)

If you leave the User ID **blank** and press the **Find** button, you will get a list of all the available users in the same domain as the DIGIPASS. The usernames are partly searchable too.

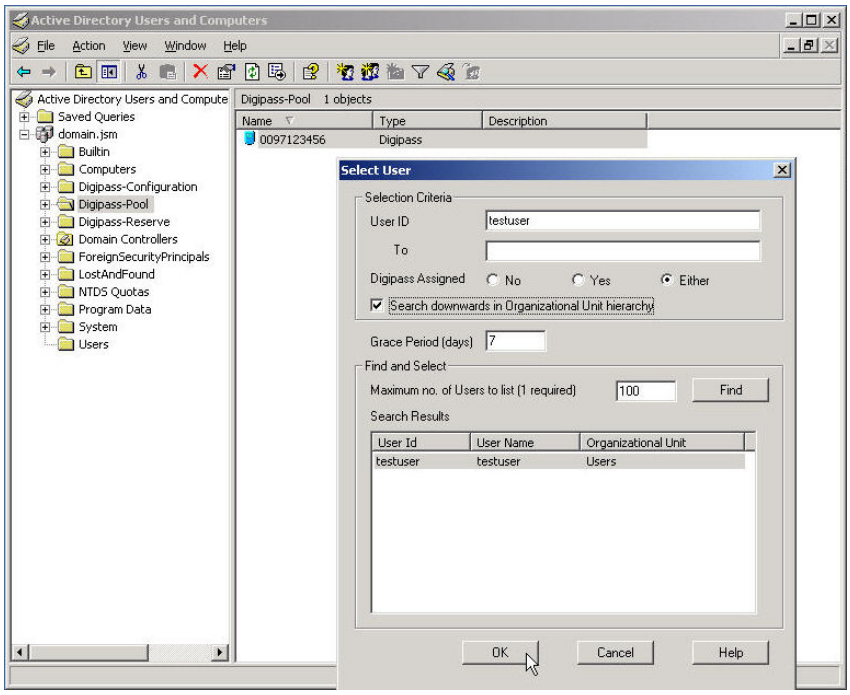


Figure 77: DIGIPASS Assignment (4)

When assigning a DIGIPASS to a user the same procedure will be applicable. You can either select the desired option to search for a DIGIPASS or through serial number. Leaving all options blank will show you all possibilities. Remember to check the "**Search upwards …**" checkbox.

9 Firebox Authentication Test

Before you will be able to logon with a known AD user, you will have to create the right global security group in AD. Also make sure the users you are trying to authenticate have Allow access enabled on the Dial-in tab of their user properties set.

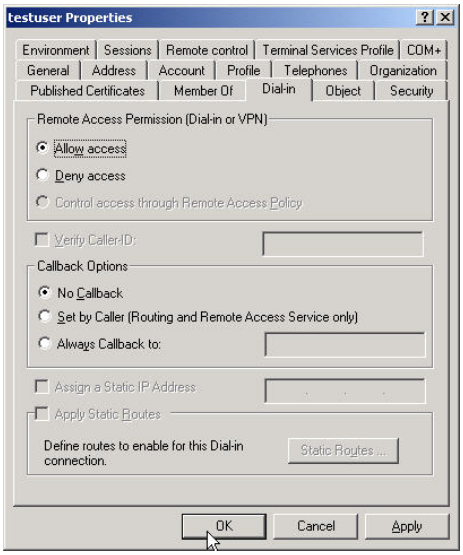


Figure 78: User properties

We will first try to gain access to the corporate website without authenticating to the Firebox.

Point your browser to the corporate website.
In our example this is http://62.58.226.226/

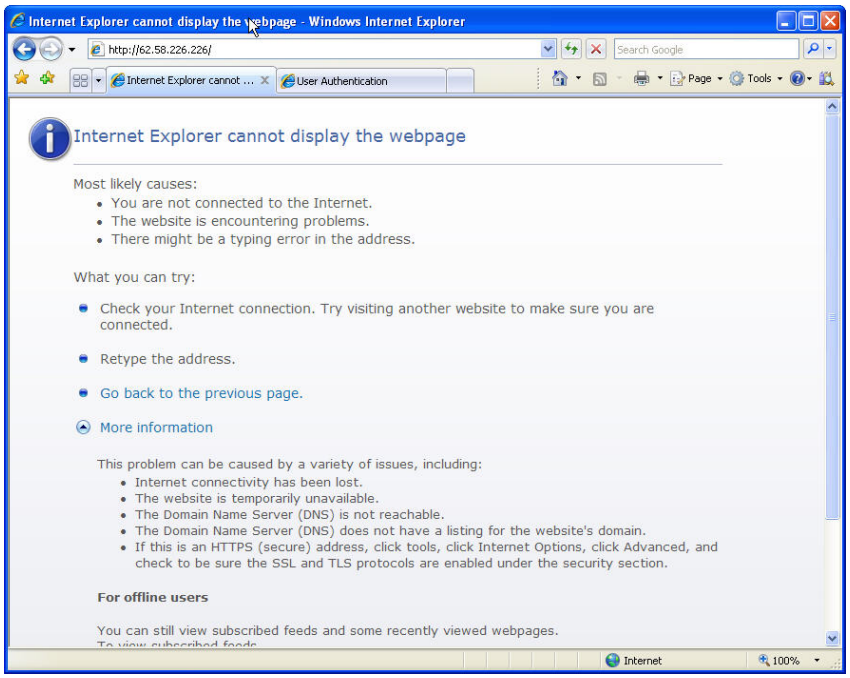

Internet Explorer cannot display the webpage - Windows Internet Explorer
http://62.58.226.226/
Search Google
Internet Explorer cannot ...
User Authentication
Page
Tools
Internet Explorer cannot display the webpage
Most likely causes:
You are not connected to the Internet.
The website is encountering problems.
There might be a typing error in the address.
What you can try:
Check your Internet connection. Try visiting another website to make sure you are connected.
Retype the address.
Go back to the previous page.
More information
This problem can be caused by a variety of issues, including:
Internet connectivity has been lost.
The website is temporarily unavailable.
The Domain Name Server (DNS) is not reachable.
The Domain Name Server (DNS) does not have a listing for the website's domain.
If this is an HTTPS (secure) address, click tools, click Internet Options, click Advanced, and check to be sure the SSL and TLS protocols are enabled under the security section.
For offline users
You can still view subscribed feeds and some recently viewed webpages.
Internet
100%

Figure 79: Firebox Authentication Test

As you could have guessed, we are not able to see the website.

9.1 Response Only

To authenticate, point your web browser to the authentication service of the Firebox. *In our example this is https://62.58.226.225:4100/*

Login with **username**: *testuser* and **password**: a *One Time Password (OTP)*. Select **RADIUS** as authentication domain and click **Login** to continue.

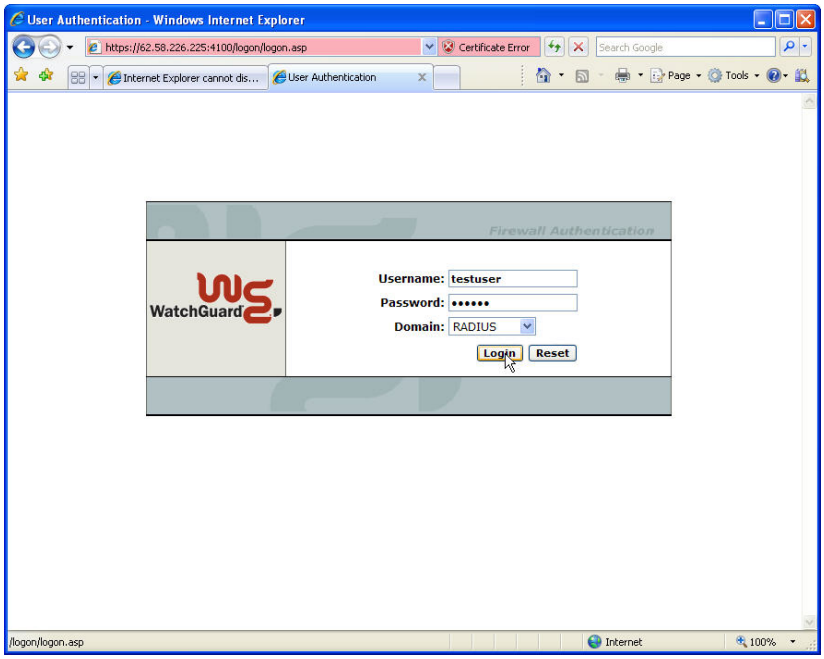


Figure 80: Response Only (1)

You will receive a message stating that the authentication was successful. The firebox remembers your IP address and username until you logout or until the session has timed out.

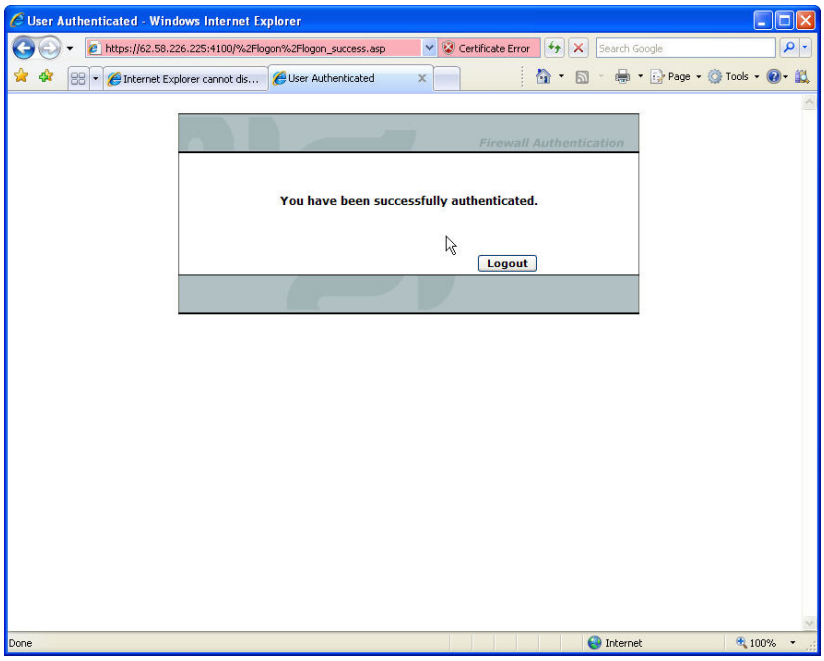


Figure 81: Response Only (2)

When we now try accessing the corporate website, you will see access is granted.

In our example this was http://62.58.226.226

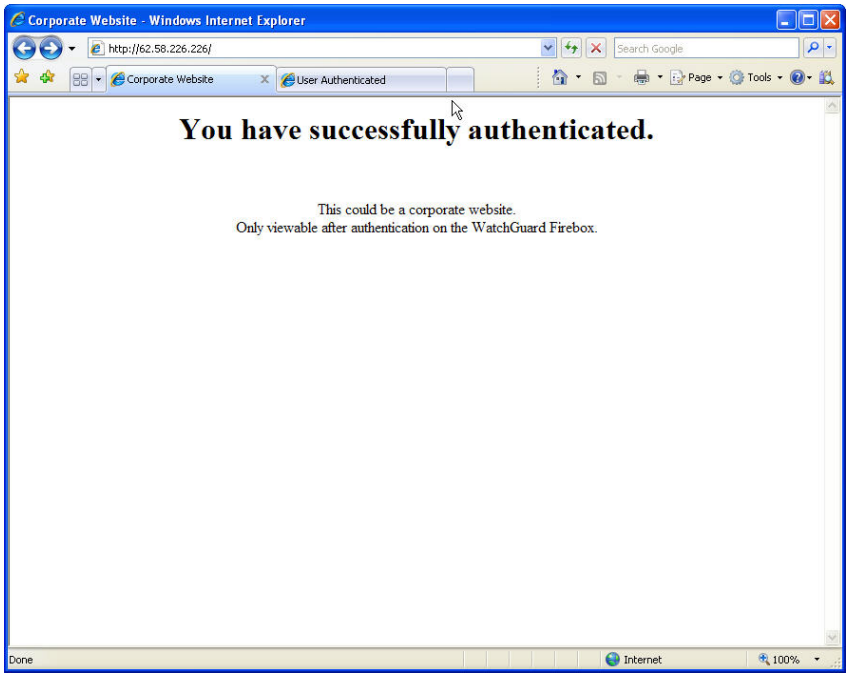


Figure 82: Response Only (3)

9.2 Challenge/Response

As we setup everything before to use “Response Only” (using only the generated OTP of a DIGIPASS), you can also use “Challenge/Response”. You only have to change one option in your policy (*Firebox Policy*) in VACMAN Middleware.

Go to the Policy properties – Challenge Settings, and select as “2-Step Challenge/Response” the option **Password**. (Make sure your DIGIPASS is out of grace period to use this method.)

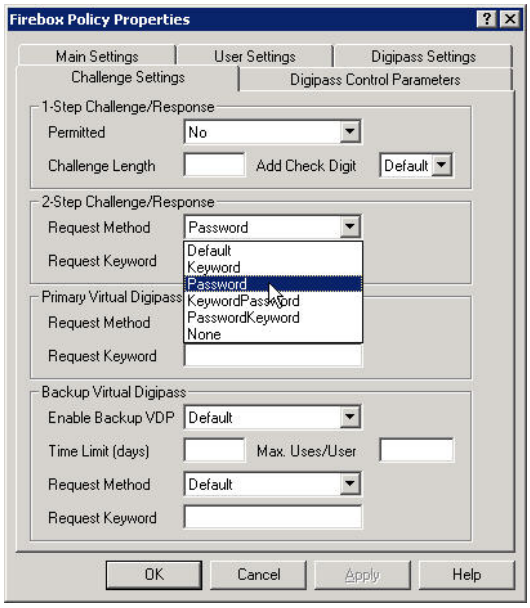


Figure 83: Challenge / Response (1)

On the login screen now type your username and password.

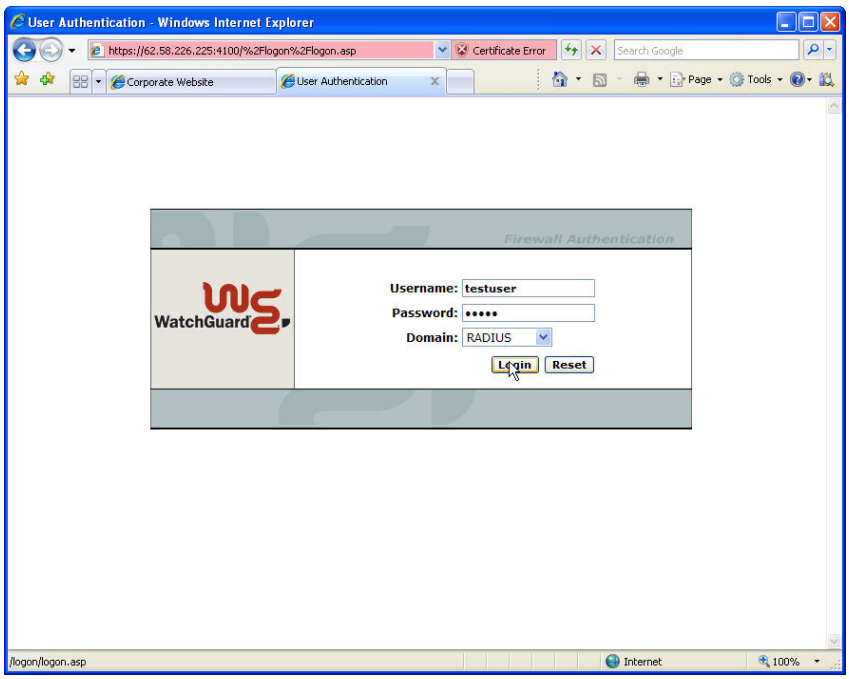


Figure 84: Challenge / Response (2)

And as you can see in **Figure 57**, the Firebox is returning you a Challenge to use on your DIGIPASS. Type the **Response** in the empty field, and click Submit.

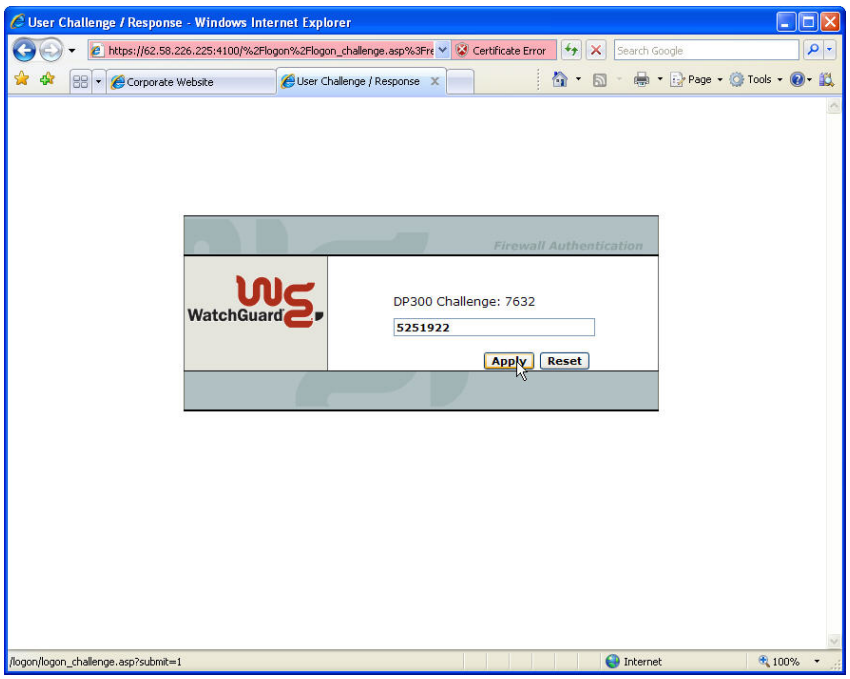


Figure 85: Challenge / Response (3)

When the authentication was successful you will receive a confirmation message on your screen. Now you can access the corporate website in a more secure way using the challenge/response method.

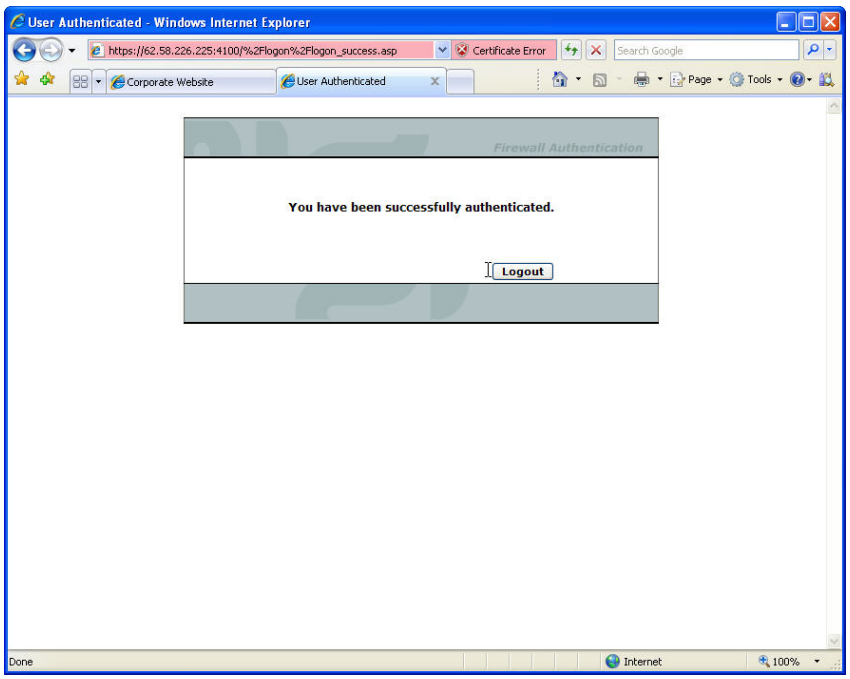


Figure 86: Challenge / Response (4)

10 VACMAN Middleware features

10.1 Installation

The VACMAN Middleware (VM) installation is very easy and straightforward. VM runs on Windows platforms, supports a variety of databases and uses an online registration. Different authentication methods allow a seamless integration into existing environments.

10.1.1 Support for Windows 2000, 2003, IIS5 and IIS6

VM can be installed on Windows 2000 and Windows 2003. Web modules exist for IIS5 and IIS 6 to protect Citrix Web Interface, Citrix Secure Gateway, Citrix Secure Access Manager (Form-based authentication), Citrix Access Gateway and Microsoft Outlook Web Access 2000 and 2003 (Basic Authentication and Form-Based Authentication).

10.1.2 Support for ODBC databases and Active Directory

Any ODBC compliant database can be used instead of the default PostgreSQL database (MS SQL Server, Oracle). Since Version 2.3 of VACMAN Middleware, AD is **not only** intended for storage of DIGIPASS anymore, but configuration and management of your DIGIPASS infrastructure is now also full integrated into the AD management tools. This option requires an AD schema update.

10.2 Deployment

Several VACMAN Middleware features exist to facilitate deployment. Combining these features provides different deployment scenarios from manual to fully automatic.

10.2.1 Dynamic User Registration (DUR)

This feature allows VM to check a username and password not in the database with a back-end RADIUS server or a Windows domain controller and, if username and password are valid, to create the username in the VM database.

10.2.2 Autolearn Passwords

Saves administrators time and effort by allowing them to change a user's password in one location only. If a user tries to log in with a password that does not match the password stored in the VM database, VM can verify it with the back-end RADIUS server or the Windows domain controller and, if correct, store it for future use.

10.2.3 Stored Password Proxy

Allows VM to save a user's RADIUS server password or Windows domain controller password in the database (static password). User's can then log in with only username and dynamic one-time password (OTP). If this feature is disabled, users must log in with username and static password immediately followed by the OTP.

10.2.4 Authentication Methods

Different authentication methods can be set on server level and on user level: local authentication (VM only), Back-End authentication (Windows or RADIUS). On top of that a combination of local and back-end can be configured. The additional parameters 'always', 'if needed' and 'never' offers you additional customization of the back-end authentication process.

The configuration of authentication methods is done within the policy (policies).

10.2.5 Policies

Policies specify various settings that affect the User authentication process. Each authentication request is handled according to a Policy that is identified by the applicable Component record. Components can be radius clients, authentication servers or Citrix web interfaces.

10.2.6 DIGIPASS Self Assign

Allows users to assign DIGIPASS to themselves by providing the serial number of the DIGIPASS, the static password and the OTP.

10.2.7 DIGIPASS Auto Assign

Allows automatic assignment of the first available DIGIPASS to a user on user creation.

10.2.8 Grace Period

Supplies a user with a certain amount of time (7 days by default) between assignment of a DIGIPASS and the user being required to log in using the OTP. The Grace Period will expire automatically on first successful use of the DIGIPASS.

10.2.9 Virtual DIGIPASS

Virtual DIGIPASS uses a text message to deliver a One Time Password to a User's mobile phone. The User then logs in to the system using this One Time Password.

Primary Virtual DIGIPASS

A Primary Virtual DIGIPASS is handled similarly to a standard physical DIGIPASS. It is imported into the VACMAN Middleware database, assigned to a User, and treated by the VACMAN Middleware database as any other kind of DIGIPASS.

Backup Virtual DIGIPASS

The Backup Virtual DIGIPASS feature simply allows a User to request an OTP to be sent to their mobile phone. It is not treated as a discrete object by VACMAN Middleware, and is not assigned to Users, only enabled or disabled. It can be enabled for Users with another type of DIGIPASS already assigned, and used when the User does not have their DIGIPASS available.

10.3 Administration

10.3.1 Active Directory Users and Computers Extensions

Since VACMAN Middleware version 2.3, Managing the users and DIGIPASS can be done within the Active Directory Users and Computers section. Selecting the properties of a user, offers complete User-DIGIPASS management.

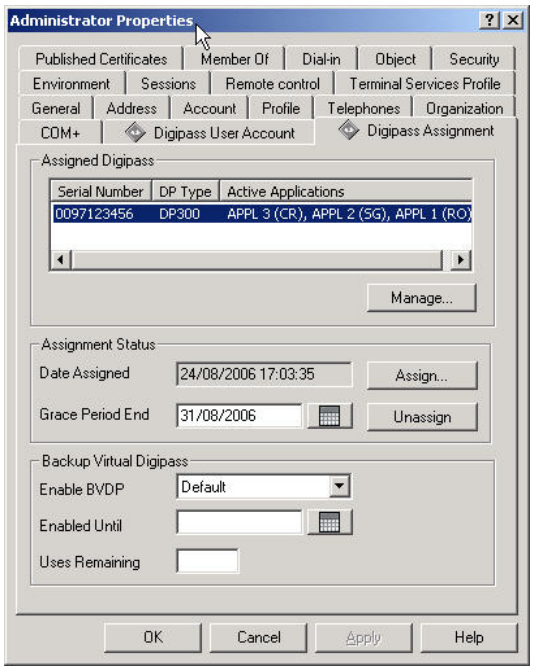


Figure 87: VM Features (1)

10.3.2 Administration MMC Interface

A highly intuitive Microsoft Management Console (MMC) exists to administer the product. An Audit Console is available to give an instant view on all actions being performed on the VM. Both can be installed on the VM server itself or on a separate PC.

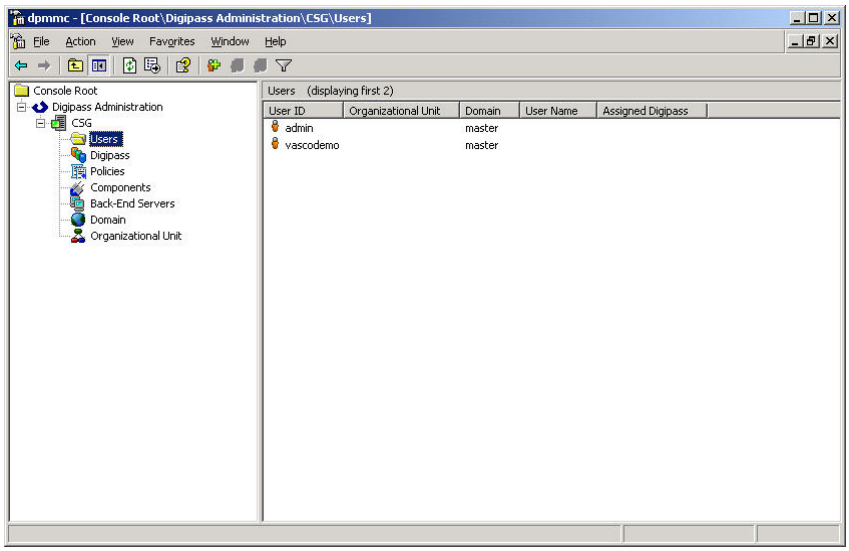


Figure 88: VM Features (2)

10.3.3 User Self Management Web Site

A web site running on IIS has been developed to allow users to register themselves to the VM with their username and back-end (RADIUS or Windows) password, to do a DIGIPASS self assign, to update their back-end password stored in the VM database, to do a change PIN (Go-1/Go-3 DIGIPASS), to do a DIGIPASS test.

Menu
User Registration
Digipass Assignment
Password Synchronization
PIN Change
Login Test
Digipass Self Service
Digipass Self Service
Welcome to the Digipass Self Service web site. Please help yourself to the following options:
User Registration
Register to receive a Digipass
Digipass Assignment
Assign a Digipass to yourself
Password Synchronization
Synchronize a new static password
Digipass PIN Change
Change your PIN for a Digipass such as the Go 1 or Go 3, or choose a PIN the first time you use the Digipass or after the PIN has been reset
Digipass Login Test
Test out your Digipass login

Figure 89: VM Features (3)

10.3.4 Delegated administration

Administration can be delegated by appointing different administrators per organizational unit (OU). These administrators can only see the DIGIPASS and users that were added to his OU.

10.3.5 Granular access rights

It is possible in VACMAN Middleware to setup different permission per user. This can be in function of a domain or an organizational unit. Administrators belonging to the Master Domain may be assigned administration privileges for all domains in the database, or just their own domain. Administrators belonging to any other Domain will have the assigned administration privileges for that Domain only.

It's possible to set different operator access levels.
E.g. A user can be created that only has the rights to unlock a DIGIPASS.

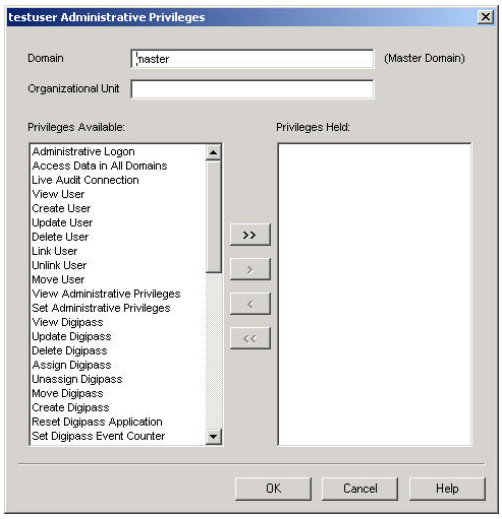


Figure 90: VM Features (4)

11 About VASCO Data Security

VASCO designs, develops, markets and supports patented Strong User Authentication products for e-Business and e-Commerce.

VASCO's User Authentication software is carried by the end user on its DIGIPASS products which are small "calculator" hardware devices, or in a software format on mobile phones, other portable devices, and PC's.

At the server side, VASCO's VACMAN products guarantee that only the designated DIGIPASS user gets access to the application.

VASCO's target markets are the applications and their several hundred million users that utilize fixed password as security.

VASCO's time-based system generates a "one-time" password that changes with every use, and is virtually impossible to hack or break.

VASCO designs, develops, markets and supports patented user authentication products for the financial world, remote access, e-business and e-commerce. VASCO's user authentication software is delivered via its DIGIPASS hardware and software security products. With over 25 million DIGIPASS products sold and delivered, VASCO has established itself as a world-leader for strong User Authentication with over 500 international financial institutions and almost 3000 blue-chip corporations and governments located in more than 100 countries.